Universitat Autònoma de Barcelona

FACULTAT DE CIÈNCIES

DEPARTAMENT DE MATEMÀTIQUES

TREBALL FINAL DE GRAU

SOBRE FORMES QUADRÀTIQUES BINÀRIES I GRUP DE CLASSES

Tutor: Francesc Bars Cortina

Helena Vila Crespo

Grau de Matemàtiques

Curs acadèmic 2021-2022

Agraïments

Agraeixo a en Francesc Bars el temps, la dedicació i la paciència tant en la preparació com en la confecció i correcció d'aquest treball final de grau.

També vull agrair el suport de la meva família i les meves companyes per acompanyar-me i ajudar-me durant aquests mesos.

Resum

Un problema clàssic de teoria de nombres és el grup de classes d'una extensió $K/\mathbb{Q}$ finita sobre $\mathbb{Q}$, és a dir, el grup abelià dels "ideals de l'anell d'enters"de K mòdul ideals principals de l'anell. Quan l'extensió és de grau 2 sobre $\mathbb{Q}$ està en bijecció amb formes quadràtiques binàries amb certes propietats, en aquest treball ens centrem en cossos quadràtics imaginaris. A *Disquisitiones arithmeticae*, Gauss ja estudia les formes quadràtiques binàries, en defineix una relació d'equivalència i una operació per formar un grup abelià finit, el grup de formes quadràtiques binàries amb unes propietats concretes, que serà isomorf al grup de classes d'una extensió de grau 2 sobre $\mathbb{Q}$. Dirichlet segueix la línia de Gauss i fa un estudi més específic i acotat sobre el grup de classes de formes i el relaciona amb el grup de classes d'ideals d'un cos quadràtic imaginari. Aquest treball té l'objectiu d'estudiar aquesta part de la teoria de nombres per veure i comprovar els resultats lligats amb el grup de classes. Un cop enllestida aquesta primera part s'ha volgut mostrar com les formes quadràtiques binàries, l'estudi d'aquestes i de les seves propietats, són útils per a altres àrees de les matemàtiques com la geometria complexa, on aprofundint trobem relacions amb superfícies abelianes (esboç en el treball), amb superfícies K3 i interrelació amb la física relativista (aquests últims punts no estan desenvolupats, veieu: [1], [12]).

Abstract

A classic number theory problem is the class group of a finite $K/\mathbb{Q}$ extension over $\mathbb{Q}$, that is, the abelian group of the "ideals of the ring of integers" of K modulus principal ideals of the ring. When the extension is of degree 2 on $\mathbb{Q}$ is in bijection with binary quadratic forms with certain properties, in this bachelor thesis we focus on imaginary quadratic fields. In *Disquisitiones arithmeticae*, Gauss already studies binary quadratic forms, defines an equivalence relation and an operation to form a finite abelian group, the group of binary quadratic forms with specific properties, which will be isomorphic to the class group of a degree 2 extension over $\mathbb{Q}$. Dirichlet follows Gauss's line of study, makes a more specific and limited study of the class group of forms, and relates it to the class group of ideals of an imaginary quadratic field. This bachelor thesis aims to study this part of number theory to see and check the results related to the class group. Once this first part has been completed, the aim is to show how binary quadratic forms, the study of these and their properties, are useful for other areas of mathematics such as complex geometry, where in-depth we find relationships with abelian surfaces (sketch in the bachelor thesis), with K3 surfaces and interrelation with relativistic physics (these last points are not developed, see: [1], [12]).

Índex

1 Formes quadràtiques binàries enteres

1.1 El conjunt de les formes quadràtiques binàries enteres amb discriminant negatiu

Per completar aquesta secció s'han utilitzat de guia les referències [1], [2], [3], [4], [5], [6] i [14].

A $\mathbb{Z}$, una expressió $f(x,y) = ax^2 + bxy + cy^2$ on $f(x,y) \in \mathbb{Z}[x,y]$ i $a,b,c \in \mathbb{Z}$ diem que és una *forma quadràtica binària* sobre $\mathbb{Z}$ amb x, y com a variables.

L'ojectiu d'aquesta secció és veure que podem definir un grup abelià finit on els seus elements són formes quadràtiques amb una operació entre elles. D'ara endavant, quan parlem de formes quadràtiques, ho farem simplement referint-nos a elles com a **formes**.

Definició 1.1.1. Diem que una forma $ax^2+bxy+cy^2$, amb $a,b,c \in \mathbb{Z}$, és *primitiva* si els coeficients a, b i c són coprimers dos a dos.

Definició 1.1.2. Definim el *discriminant* de $f(x,y) = ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ com $D = b^2 - 4ac$.

Observem que una forma la podem escriure matricialment com $f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. Calculem els valors propis de la matriu simètrica $B = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ i obtenim $\lambda = \frac{(a+c) \pm \sqrt{(a+c)^2+D}}{2}$, que són tots reals pel teorema espectral. Diem que una matriu B és *definida* si els seus valors propis tenen el mateix signe i *indefinida* en cas contrari.

Fem el producte dels valors propis de B:

$$\left(\frac{(a+c)+\sqrt{(a+c)^2+D}}{2}\right) \cdot \left(\frac{(a+c)-\sqrt{(a+c)^2+D}}{2}\right) = -\frac{D}{4}$$

de manera que si $D > 0$ la matriu serà indefinida i si $D < 0$, definida. A partir d'aquesta observació, podem definir el següent:

1. Si $D > 0$, diem que $f(x,y)$ és una forma *indefinida* ja que pot representar enters tant positius com negatius, és a dir $\{f(x,y)|x,y \in \mathbb{Z}\} \cap \mathbb{Z} \subsetneq \{f(x,y)|x,y \in \mathbb{Z}\} \cap \mathbb{N}$.

2. Si $D < 0$, diem que $f(x,y)$ és una forma *definida* donat que representa únicament enters positius, en aquest cas direm que és *definida positiva*, i $a > 0$, o bé enters negatius, amb $a < 0$ i diem *definida negativa*.

De la definició de discriminant observem:

$$D = b^2 - 4ac \Longrightarrow D \equiv b^2 \pmod 4$$

fet que ens permet reduir D a dos únics casos. Si b és parell aleshores $D \equiv 0 \pmod 4$, si b és senar $D \equiv 1 \pmod 4$.

Definició 1.1.3. Una forma primitiva definida positiva $ax^2 + bxy + cy^2$ diem que és *reduïda* si

$$|b| \leq a \leq c \tag{1.1}$$

sempre i quan no hi hagi igualtats. Quan ens trobem una forma reduïda amb alguna igualtat en (1.1) suposem que $b \geq 0$ amb $|b| = a$ ó $a = c$.

Definició 1.1.4. Diem que dues formes $f(x, y)$ i $g(x, y)$ són *equivalents* si $\exists p, q, r, s \in \mathbb{Z}$ tals que

$$f(x, y) = g(px + qy, rx + sy) \text{ amb } ps - qr = \pm 1.$$

Matricialment, escrivim $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i tenim $f(x, y) = g(A \begin{pmatrix} x \\ y \end{pmatrix}) = g(px + qy, rx + sy)$ i $det(A) = \pm 1$, on $A \in GL_2(\mathbb{Z})$.

Diem que $f(x, y)$ i $g(x, y)$ són *pròpiament equivalents* si són equivalents amb $ps - qr = 1$, en aquest cas $A \in SL_2(\mathbb{Z})$.

Lema 1.1.1. *Dues formes equivalents f i g tenen el mateix discriminant D.*

Demostració. Siguin $f(x, y) = a_1x^2 + b_1xy + c_1y^2$ i $g(x, y) = a_2x^2 + b_2xy + c_2y^2$ formes equivalents. Escrivim $f(x, y) = g(px + qy, rx + sy)$ amb $p, q, r, s \in \mathbb{Z}$. Volem comprovar que $b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = D$.

- Substituïm directament amb la definició d'equivalència: $f(x, y) = g(px + qy, rx + sy) = (a_2p^2 + b_2pr + c_2r^2)x^2 + (2a_2pq + b_2qr + b_2ps + 2c_2rs)xy + (a_2q^2 + b_2qs + c_2s^2)$.

  Per tant tenim les següents igualtats:

$$\begin{aligned} a_1 &= a_2p^2 + b_2pr + c_2r^2 \\ b_1 &= 2a_2pq + b_2qr + b_2ps + 2c_2rs \\ c_1 &= a_2q^2 + b_2qs + c_2s^2 \end{aligned} \tag{1.2}$$

- Calculem ara $b_1^2 - 4a_1c_1$ substituint pels valors equivalents:

$$b_1^2 - 4a_1c_1 = (p^2s^2 - 2pqrs + q^2r^2)(b_2^2 - 4a_2c_2) = (ps - qr)^2(b_2^2 - 4a_2c_2) = b_2^2 - 4a_2c_2$$

  ja que $ps - qr = \pm 1$

Hem vist que si dues formes són equivalents, aleshores tenen el mateix discriminant.

□

Exemple 1.1.2. *Donades $f(x, y) = x^2 - 2xy + 6y^2$ i $g(x, y) = x^2 + 5y^2$, si prenem $A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ podem comprovar amb un càlcul que $g(A \begin{pmatrix} x \\ y \end{pmatrix}) = f(x, y)$. Observem que $D_f = (-2)^2 - 4 \cdot 1 \cdot 6 = -20 = 0^2 - 4 \cdot 1 \cdot 5 = D_g$, on D_h denota el discriminant de la forma h, i $\det(A) = 1$, per tant, f i g són dues formes pròpiament equivalents amb el mateix discriminant.*

Teorema 1.1.3. *Tota forma primitiva definida positiva és pròpiament equivalent a una única forma reduïda.*

Demostració. • Veurem que donada una forma primitiva definida positiva, aquesta és pròpiament equivalent a una forma complint $|b| \leq a \leq c$.

Considerem una forma primitiva definida positiva i, de totes les que són pròpiament equivalents, prenem $f(x,y) = ax^2 + bxy + cy^2$ tal que $|b|$ és el més petit possible.

Si $a < |b|$, considerem $g(x,y) = f(x + my, y) = ax^2 + (2am + b)xy + c'y^2$, que és clarament equivalent a f. En aquest cas, podem escollir $m \in \mathbb{Z}$ tal que $|2am + b| < |b|$, perque $[-b, b]$ té $2b + 1$ enters i $h(x) = 2ax + x$ té un enter en $(-b, b)$, fet que contradiu l'elecció de f; per tant tenim $|b| \leq a$. Per demostrar $|b| \leq c$ seguim el mateix raonament. Suposem $c < |b|$ i considerem $g(x,y) = f(x, mx + y) = a'x^2 + (2cm + b)xy + cy^2$, escollim $m \in \mathbb{Z}$ tal que $|2cm + b| < |b|$ i trobem una contradicció. Veiem ara $a \leq c$. Si tenim $a > c$ i fem $(x,y) \mapsto (-y, x)$, obtenim una forma pròpiament equivalent que compleix $|b| \leq a \leq c$.

- El següent pas és veure que $f(x,y)$ amb $|b| \leq a \leq c$ és pròpiament equivalent a una forma reduïda. Per definició, aquesta forma ja és reduïda excepte que $b < 0$ i $a = -b$ o bé $a = c$. Demostrem que $ax^2 + bxy + cy^2$ i $ax^2 - bxy + cy^2$ són pròpiament equivalents:

  Si $a = -b$, considerem $(x,y) \mapsto (x+y, y)$ de manera que $ax^2 - axy + cy^2 \mapsto ax^2 + axy + cy^2$ que són pròpiament equivalents. Pel cas $a = c$ considerem $(x,y) \mapsto (-y, x)$ i $ax^2 + bxy + ay^2 \mapsto ax^2 - bxy + ay^2$ que també ho és. Per tant, $f(x,y)$ és reduïda si $b \geq 0$, i si $b < 0$ amb $a = -b$ o $a = c$, aleshores $ax^2 - bxy + cy^2$ és reduïda.

- Seguidament veiem que dos formes reduïdes no poden ser pròpiament equivalents. Per simplificar, considerem $f(x,y) = ax^2 + bxy + cy^2$ una forma reduïda que compleix les desigualtats estrictes: $|b| < a < c$. Per demostrar-ho, veurem primer quins són els tres valors no trivials més petits representats per f. Observem que si $xy = 0$ aleshores:

$$f(1,0) = a$$
$$f(0,1) = c$$

  Si, en canvi, $xy \neq 0$ hi ha els següents possibles casos:

  1. si $xy > 0$ i $b > 0 \implies xy \geq min(x^2, y^2), x^2 \geq min(x^2, y^2)$ i $y^2 \geq min(x^2, y^2) \implies f(x,y) = ax^2 + bxy + cy^2 \geq (a + b + c)min(x^2, y^2)$
  2. si $xy < 0$ i $b < 0 \implies |xy| \geq min(x^2, y^2), x^2 \geq min(x^2, y^2)$ i $y^2 \geq min(x^2, y^2) \implies f(x,y) = ax^2 + |b||xy| + cy^2 \geq (a + |b| + c)min(x^2, y^2)$
  3. si $xy > 0$ i $b < 0 \implies xy \geq min(x^2, y^2), x^2 \geq min(x^2, y^2)$ i $y^2 \geq min(x^2, y^2) \implies f(x,y) = ax^2 - |b|xy + cy^2 \geq (a - |b| + c)min(x^2, y^2)$
  4. si $xy < 0$ i $b > 0 \implies |xy| \geq min(x^2, y^2), x^2 \geq min(x^2, y^2)$ i $y^2 \geq min(x^2, y^2) \implies f(x,y) = ax^2 - |b||xy| + cy^2 \geq (a - |b| + c)min(x^2, y^2)$

  Per tant, en general tenim $f(x,y) \geq a - |b| + c$ si $xy \neq 0$ i podem dir que $a < c < a - |b| + c$ són els valors més petits representats per f. També podem observar que:

$$\begin{aligned} f(x,y) = a, mcd(x,y) = 1 &\iff (x,y) = \pm(1,0) \\ f(x,y) = c, mcd(x,y) = 1 &\iff (x,y) = \pm(0,1) \end{aligned} \tag{1.3}$$

  Considerem ara $g(x,y) = a'x^2 + b'xy + c'y^2$ una forma reduïda pròpiament equivalent a $f(x,y)$. Per equivalència, f i g representen els mateixos valors, per tant, el primer coeficient a és el mateix ($a = a'$). g és una forma reduïda, aleshores $a \leq c'$. Si tenim la igualtat, l'equació $g(x,y) = a$ té quatre possibles solucions $\pm(1,0)$ i $\pm(0,1)$, però f és pròpiament equivalent a

g i per (1.3) arribem a contradicció. Veiem ara que sabent $a < c'$, tenim $c = c'$. $g(x, y)$ és una forma reduïda, per tant $|b'| < a < c'$, alhora es compleix $a < c' < a - |b'| + c'$. Observem que $g(x, y) = c', mcd(x, y) = 1 \implies xy = 0$ ja que si $xy \neq 0$, tenim $g(x, y) > a, g(x, y) > c'$ que són els valors més petits representats per g. Però f i g respresenten els mateixos valors per equivalència i els valors més petits representats per f són $\{a, c\}$, de manera que $\{a, c\} = \{a, c'\} \implies c = c'$.

Per equivalència, Lema 1.1.1, f i g tenen el mateix discriminant:

$$b^2 - 4ac = b'^2 - 4ac \implies b = \pm b'$$

i podem escriure g com $g(x, y) = ax^2 \pm bxy + cy^2$.

Per acabar veiem que $f(x, y) = g(x, y)$. Sabem que són pròpiament equivalents, per tant, $\exists p, q, r, s \in \mathbb{Z}$ tals que $g(x, y) = f(px + qy, rx + sy)$ amb $ps - qr = 1$. A més, tenim que:

$$g(1, 0) = f(p, r) = a$$
$$g(0, 1) = f(q, s) = c$$

són representacions propies i per (1.3) $(p, r) = \pm(1, 0)$, $(q, s) = \pm(0, 1)$ i $ps - qr = 1 \implies \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Per tant, $f(x, y) = g(x, y)$.

- Si en comptes de considerar les desigualtats estrictes $|b| < a < c$ per f considerem $a = c$ tenim $f(x, y) = ax^2 + bxy + ay^2$ i $g(x, y) = a'x^2 + b'xy + c'y^2$. Pel raonament utilitzat al punt anterior de la demostració podem dir que $a = a'$ i per equivalència tenim $g(x, y) = ax^2 + b'xy + ay^2$. Sabem que el discriminant de les dues formes és el mateix:

$$b^2 - 4a^2 = b'^2 - 4a^2 \implies b^2 = b'^2 \implies b = \pm b'$$

Reescrivim $g(x, y) = ax^2 \pm bxy + ay^2$ i per equivalència podem concloure que $f = g$.

Pel cas $|b| = a$ podem prendre $b \geq 0$ i seguint el mateix procediment tenim $f(x, y) = ax^2 + axy + cy^2$ i $g(x, y) = ax^2 + axy + c'y^2$. Volem veure $c = c'$. Observem el següent:

$$f(x, y) = a \iff (x, y) = \pm(1, 0)$$
$$f(x, y) = c \iff (x, y) = \pm(0, 1) \text{ o bé } (x, y) = \pm(1, -1)$$

Per les equacions $g(x, y) = a$ i $g(x, y) = c$ tenim les mateixes solucions. Si considerem el canvi $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ tenim $c = c'$. Però si considerem $\pm \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ tenim:

$$f(x + y, -y) = a(x + y)^2 + a(x + y)(-y) + c(-y)^2 = ax^2 - axy + cy^2$$

que no pot ser ja que $\det(\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}) = -1$ i no obtenim equivalència pròpia. Per tant, l'única possibilitat és el canvi $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ que implica $f(x, y) = g(x, y)$.

□

Definició 1.1.5. Donada la relació d'equivalència pròpia definim les *classes* de formes primitives definides positives com les classes d'equivalència de la relació pròpiament equivalents.

Si $D < 0$, prenem com a representants les formes reduïdes pel Teorema 1.1.3.

Definició 1.1.6. Definim $h(D)$ com el número de les classes diferents de formes primitives definides positives de discriminant fixat D.

Definim $C(D)$ com el conjunt d'aquestes classes de formes de discriminant D mòdul equivalència de pròpiament equivalents.

Pel Teorema 1.1.3, si $D < 0$, $h(D)$ és igual al nombre de formes reduïdes de discriminant D.

Teorema 1.1.4. *Donat un $D < 0$, aleshores $h(D)$ és finit.*

Demostració. Si $ax^2+bxy+cy^2$ és una forma reduïda de discriminant $D < 0$, aleshores es compleix que $b^2 \leq a^2$ i $a \leq c$ i per tant $-D = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2 \Longrightarrow a \leq \sqrt{\frac{-D}{3}}$; D és fixat i $|b| \leq a$ de manera que tenim un nombre finit d'eleccions per a i b.

Com que $b^2 - 4ac = D$, tenim el mateix per c i podem dir que hi ha un nombre finit de formes reduïdes de discriminant D. Per l'esmentat anteriorment, això implica que el nombre de classes de formes pròpiament equivalents és finit. □

El codi de Magma de l'Apèndix A ens proporciona un algorisme que, donat $D < 0$ fixat, calcula el nombre de classes d'aquest discriminant i les formes reduïdes associades. A l'Apèndix C també hi trobareu una taula de les formes reduïdes per a alguns $D < 0$ fixats.

Observació 1.1. *Cal esmentar que existeix una teoria corresponent per a formes indefinides ($D > 0$). Fermat i Euler inicien aquesta teoria però Lagrange i Gauss van desenvolupar una teoria general d'aquestes formes. Hi ha nocions de forma reduïda, número de classes, etc. però el problema d'unicitat és molt més complicat. Gauss observa que per $D > 0$ hi ha formes reduïdes pròpiament equivalents entre elles, però determinar exactament quines formes són aquestes no és fàcil. El lector interessat pot consultar [2].*

1.2 Grup de classes

Per obrir aquesta secció, presentem la següent identitat atribuïda al matemàtic indi Brahmagupta (598–668 dC.).

Proposició 1.2.1. *Per a enters x, y, z, w, D qualssevol,*

$$(x^2 + Dy^2)(z^2 + Dw^2) = (xz - Dyw)^2 + D(xw + zy)^2$$

Demostració. Només cal desenvolupar els productes i es veu fàcilment que aquesta identitat es compleix. □

Exemple 1.2.2. *Si prenem $D = -4$*

$$(x^2 - 4y^2)(z^2 - 4w^2) = x^2z^2 - 4x^2w^2 - 4y^2z^2 + 16y^2w^2 =$$

$$= (x^2z^2 + 16y^2w^2 - 8xyzw) + (8xyzw - 4x^2w^2 - 4y^2z^2) = (xz - 4yw)^2 - 4(xw + yz)^2$$

Hem vist un exemple de la identitat de Brahmagupta per un D fixat.

Aquesta identitat ens permet dir que els nombres de la forma $x^2 + Dy^2$ són tancats sota multiplicació. Gauss es va preguntar si era possible generalitzar-ho a formes quadràtiques binàries, és a dir, $ax^2 + bxy + cy^2$.

Donades $f(x, y)$ i $g(x, y)$ formes de discriminant $D < 0$, volem definir la forma $F(x, y)$ que anomenarem *composició* de f i g de la següent manera:

$$f(x, y) * g(z, w) := F(B_1(x, y; z, w), B_2(x, y; z, w))$$

on $B_i(x,y;z,w) = a_i xz + b_i xw + c_i yz + d_i yw$, $i = 1,2$ són formes bilineals en x,y i z,w i F ha de ser una forma amb discriminant D.

Gauss busca, donades f i g dues formes de discriminant $D < 0$, trobar una transformació

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix} \tag{1.4}$$

amb $p_i, q_i \in \mathbb{Z}$ per $i = 0, \ldots, 3$ i enters A, B, C, complint:

$$f(x,y) * g(z,w) = AX^2 + BXY + CY^2 \tag{1.5}$$

amb $B^2 - 4AC = D$. Vol estudiar què passa per a formes equivalents suposant que aquesta transformació existeix.

Buscarem composicions d'aquest tipus.

Observació 1.2. *Donades f, g formes i $f * g = F$ on F descrit via (1.5), considerem $f \sim f'$ i $g \sim g'$ on $\sim$ pròpiament equivalents, prenem $M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ i $M_2 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ en $SL_2(\mathbb{Z})$ dos canvis de variable*

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = M_1 \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} z' \\ w' \end{pmatrix} = M_2 \begin{pmatrix} z \\ w \end{pmatrix}$$

Busquem ara la matriu M del canvi

$$\begin{pmatrix} x'z' \\ x'w' \\ y'z' \\ y'w' \end{pmatrix} = M \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$$

Tenim

$$\begin{array}{rcl} x' = ax + by & & x'z' = aexz + afxw + beyz + bfyw \\ y' = cx + dy & \Longrightarrow & x'w' = agxz + ahxw + bgyz + bhyw \\ z' = ez + fw & & y'z' = cexz + cfxw + deyz + dfyw \\ w' = gz + hw & & y'w' = cgxz + chxw + dgyz + dhyw \end{array}$$

per tant

$$M = \begin{pmatrix} ae & af & be & bf \\ ag & ah & bg & bh \\ ce & cf & de & df \\ cg & ch & dg & dh \end{pmatrix} = (M_1 \otimes M_2)$$

on $\otimes$ és el producte de Kronecker.

Observem que $det(M) = det(M_1 \otimes M_2) = det(M_1)^2 det(M_2)^2 = 1$ per propietats del producte de Kronecker i per tant M és una matriu de canvi de variable. Escrivim

$$\begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix} = M^{-1} \begin{pmatrix} x'z' \\ x'w' \\ y'z' \\ y'w' \end{pmatrix}.$$

Si $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$ *i* $f'(x', y') = f(M_1 \begin{pmatrix} x \\ y \end{pmatrix})$ *i* $g'(z', w') = g(M_2 \begin{pmatrix} z \\ w \end{pmatrix})$. *Tenim*

$$F(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} A \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} xz & xw & yz & yw \end{pmatrix} \begin{pmatrix} p_0 & q_0 \\ p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{pmatrix} A \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix} =$$

$$= \begin{pmatrix} x'z' & x'w' & y'z' & y'w' \end{pmatrix} (M^{-1})^T \begin{pmatrix} p_0 & q_0 \\ p_1 & q_1 \\ p_2 & q_2 \\ p_3 & q_3 \end{pmatrix} A \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} M^{-1} \begin{pmatrix} x'z' \\ x'w' \\ y'z' \\ y'w' \end{pmatrix}$$

Posant $\begin{pmatrix} p'_0 & p'_1 & p'_2 & p'_3 \\ q'_0 & q'_1 & q'_2 & q'_3 \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} M^{-1}$ *i definint* $\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} p'_0 & p'_1 & p'_2 & p'_3 \\ q'_0 & q'_1 & q'_2 & q'_3 \end{pmatrix} \begin{pmatrix} x'z' \\ x'w' \\ y'z' \\ y'w' \end{pmatrix}$

trobem

$$F(X,Y) = F(X',Y')$$

Suposant que existeix la matriu $\begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix}$ *tal que* $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$,

hem vist com es comporta el canvi de variable en la composició.

Observació 1.3. *El producte de Kronecker és una operació de matrius definida com:*

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \otimes \begin{pmatrix} b_{1,1} & \cdots & b_{1,s} \\ \vdots & \ddots & \vdots \\ b_{r,1} & \cdots & b_{r,s} \end{pmatrix} = \begin{pmatrix} a_{1,1}b_{1,1} & \cdots & a_{1,1}b_{1,s} & \cdots & \cdots & a_{1,n}b_{1,1} & \cdots & a_{1,n}b_{1,s} \\ \vdots & \ddots & \vdots & & & \vdots & \ddots & \vdots \\ a_{1,1}b_{r,1} & \cdots & a_{1,1}b_{r,s} & \cdots & \cdots & a_{1,n}b_{r,1} & \cdots & a_{1,n}b_{r,s} \\ \vdots & & \vdots & \ddots & & \vdots & & \vdots \\ \vdots & & \vdots & & \ddots & \vdots & & \vdots \\ a_{m,1}b_{1,1} & \cdots & a_{m,1}b_{1,s} & \cdots & \cdots & a_{m,n}b_{1,1} & \cdots & a_{m,n}b_{1,s} \\ \vdots & \ddots & \vdots & & & \vdots & \ddots & \vdots \\ a_{m,1}b_{r,1} & \cdots & a_{m,1}b_{r,s} & \cdots & \cdots & a_{m,n}b_{r,1} & \cdots & a_{m,n}b_{r,s} \end{pmatrix}$$

amb $a_{i,j}, b_{k,l} \in R$, *on* R *és un anell. Aquest producte té les següents propietats:*

- *Bilineal i associatiu*

$$\begin{aligned} A \otimes (B + C) &= A \otimes B + A \otimes C \\ (A + B) \otimes C &= A \otimes C + B \otimes C \\ (kA) \otimes B = A \otimes (kB) &= k(A \otimes B) \\ A \otimes (B \otimes C) &= (A \otimes B) \otimes C \\ A \otimes 0 = 0 \otimes A &= 0 \end{aligned}$$

  on A, B, C *són matrius,* $k \in \mathbb{Z}$ *i* 0 *és la matriu zero.*

- *No commutatiu*

- *Propietat del producte mixte*

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

- *Inversa*

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$$

- *Transposada*

$$(A \otimes B)^T = A^T \otimes B^T$$

- *Determinant. Siguin* $A \in M_n(R)$ *i* $B \in M_m(R)$

$$|A \otimes B| = |A|^m |B|^n$$

Veieu [13] per més detall sobre les seves propietats.

Exemple 1.2.3. *Prenem* $f(x,y) = 2x^2 + 2xy + 3y^2$ *i calculem* $F(X,Y) = f(x,y) * f(z,w)$*:*

$$(2x^2 + 2xy + 3y^2) * (2z^2 + 2zw + 3w^2) =$$

$$= 6w^2x^2 + 6w^2xy + 9w^2y^2 + 4wx^2z + 4wxyz + 6wy^2z + 4x^2z^2 + 4xyz^2 + 6y^2z^2 =$$

$$= (2xz + xw + yz + 3yw)^2 + 5(xw - yz)^2 = X^2 + 5Y^2$$

Podem definir ara la matriu M *tal que* $\begin{pmatrix} X \\ Y \end{pmatrix} = M \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$*:*

$$M = \begin{pmatrix} 2 & 1 & 1 & 3 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

Considerem ara la matriu de canvi $A = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ *i* $f'(x',y') = f(A \begin{pmatrix} x \\ y \end{pmatrix}) = f(x-y, y) = 2x^2 - 2xy + 3y^2$*. Calculem ara* $F(X',Y') = f'(x',y') * f'(z',w')$

$$(2x^2 - 2xy + 3y^2) * (2z^2 - 2zw + 3w^2) =$$

$$6w^2x^2 - 6w^2xy + 9w^2y^2 - 4wx^2z + 4wxyz - 6wy^2z + 4x^2z^2 - 4xyz^2 + 6y^2z^2$$

Per veure que com es comporta la composició per equivalències calculem M'*. Primer fem* $A \otimes A$

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Per tant

$$M' = M(A \otimes A) = \begin{pmatrix} 2 & 1 & 1 & 3 \\ 0 & 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 & -1 & 3 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

$i \begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 2xz - xw - yz + 3yw \\ xw - yz \end{pmatrix}$. *Calculem* $X'^2 + 5Y'^2$*:*

$$(2xz - xw - yz + 3yw)^2 + 5(xw - yz)^2 =$$

$$6w^2x^2 - 6w^2xy + 9w^2y^2 - 4wx^2z + 4wxyz - 6wy^2z + 4x^2z^2 - 4xyz^2 + 6y^2z^2$$

Veiem que certament $F(X, Y) = F(X', Y')$.

Volem estudiar les propietats de $*$ en (1.5).

Definició 1.2.1. Diem que dues formes (a_1, b_1, c_1) i (a_2, b_2, c_2) de discriminant D són *de Dirichlet*[1] si

$$mcd(a_1, a_2, \frac{b_1 + b_2}{2}) = 1$$

Observació 1.4. $\frac{b_1+b_2}{2}$ *és enter perquè* b_1 *i* b_2 *tenen la mateixa paritat, ja que* $D \equiv b_1^2 \equiv b_2^2 \mod 4 \Longrightarrow b_1 \equiv b_2 \mod 2$.

Donades dues formes f i g, volem trobar g' tal que $g \sim g'$ on f i g' siguin de Dirichlet.

Lema 1.2.4. *Una forma* f *representa un enter* m*, és a dir existeixen* $\alpha_1, \beta_1 \in \mathbb{Z}$ *on* $f(\alpha_1, \beta_1) = m$*, si i només si,* $f \sim (m, b, c)$ *per alguns enters* b *i* c*.*

Demostració. Suposem $f(\alpha_1, \beta_1) = m$ per certs $\alpha_1, \beta_1 \in \mathbb{Z}$ amb $mcd(\alpha_1, \beta_1) = 1$, $\exists r, s \in \mathbb{Z}$ on $s\alpha_1 + r\beta_1 = 1$. El canvi $A = \begin{pmatrix} \alpha_1 & r \\ \beta_1 & s \end{pmatrix} \in SL_2(\mathbb{Z})$

$$f(\alpha_1 x + ry, \beta_1 x + sy) = f(\alpha_1, \beta_1)x^2 + bxy + cy^2$$

per a certs b, c enters. Per veure la implicació contrària observem que $mx^2 + bxy + cy^2$ representa m prenent $(x, y) = (1, 0)$, $\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} m & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = m$.

Si fem un canvi $M \in SL_2(\mathbb{Z})$, tenim que és igual a

$$\begin{pmatrix} 1 & 0 \end{pmatrix} (M^{-1})^T M^T \begin{pmatrix} m & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} M M^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

on $f \sim (m, b, c)$ representa m amb vectors $M^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

□

Lema 1.2.5. *Una forma primitiva* $f = (a, b, c)$ *representa un enter* m *coprimer a un enter fixat* k*.*

Demostració. Denotem $Prim(n_1, n_2, n_3)$ al producte de tots els primers dividint els enters n_1, n_2, n_3 i $Prim(n_1, n_2, n_3^{\perp})$ el producte dels primers dividint n_1 i n_2 i que no divideixen n_3.

Escrivim $P_1 := Prim(k, a, c), P_2 := Prim(k, a, c^{\perp}), P_3 := Prim(k, a^{\perp}, c)$ i $P_4 := Prim(k, a^{\perp}, c^{\perp})$, aleshores

$$P_1P_2P_3P_4 = Prim(k, 0, 0)$$

on $mcd(P_i, P_j) = 1$.

Fem $f(P_2, P_3P_4) = M$, f representa l'enter M. Volem veure $mcd(M, k) = 1$ i per tant podem triar $M = m$.

[1] Aquest concepte l'introdueix Dirichlet per simplificar la composició. Dirichlet utilitza el terme *united forms* però en aquest treball ens referim a elles com *formes de Dirichlet*

Si l primer que divideix k i M, llavors l divideix M i algun P_i per $i = 1, \ldots, 4$

$$M = a(P_2)^2 + bP_2P_3P_4 + c(P_3P_4)^2$$

si $l|M$ i $l|P_2 \Longrightarrow l|c(P_3P_4)^2$ on $l|(P_3P_4)^2$ però $l \nmid c$ i $l \in P_2$, no pot ser P_3 o P_4, per tant, $l = 1$.

Per P_3 i P_4 es demostra seguint un argument similar.

Si $l|M$ i $l|P_1$, tenim $l|a$ i $l|c$ on $l|bP_2P_3P_4$ però $l \nmid b$ perquè $f = (a, b, c)$ primitiva i $l|P_2P_3P_4$, però això no pot ser, $l \in P_1$ llevat $l = 1$.

□

Corol·lari 1.2.6. *Donades $f = (a, b, c)$ i $g = (a_1, b_1, c_1)$, existeix $g' = (a_2, b_2, c_2)$ amb $g \sim g'$ i $mcd(a_1, a_2) = 1$, en particular f i g' són de Dirichlet.*

Demostració. Triem qualsevol a_2 coprimer amb a, pel lema anterior g representa a_2 i pel Lema 1.2.4 $g \sim (a_2, b_2, c_2) = g'$ per a certs b_2, c_2 enters.

□

Introduïm el següent lema:

Lema 1.2.7. *Siguin $p_1, q_1, \ldots, p_r, q_r, m$ enters amb $mcd(p_1, \ldots, p_r, m) = 1$. Aleshores les congruències*

$$p_iB \equiv q_i \ mod\ m, \quad i = 1, \ldots, r$$

tenen una única solució mòdul m si i només si, per tot $i, j = 1, \ldots, r$ tenim

$$p_iq_j \equiv p_jq_i \ mod\ m$$

Demostració.

- Comencem suposant que les congruències

$$p_iB \equiv q_i \bmod m, \quad i = 1, \ldots, r$$

tenen una única solució mòdul m. Prenem $i, j \in \{1, \ldots, r\}$ i per hipòtesi tenim

$$p_iB - q_i = ml$$
$$p_jB - q_j = ml'$$

La primera igualtat la multipliquem per p_j i la segona per p_i i les restem:

$$\left.\begin{aligned} p_jp_iB - p_jq_i &= ml_1 \\ p_ip_jB - p_iq_j &= ml_1' \end{aligned}\right\} \Longrightarrow p_jq_i - p_iq_j = mL \Longrightarrow p_iq_j \equiv p_jq_i \bmod m$$

Arribem a la congruència que buscàvem que val per $\forall i, j \in \{1, \ldots, r\}$

- Veiem ara la implicació contrària. Per hipòtesi sabem que $mcd(m, p_1, \ldots, p_r) = 1$ i per la Identitat de Bézout $\exists a, a_1, \ldots, a_r$ tals que $am + \sum_{i=1}^{r} p_ia_i = 1$.

  Volem resoldre $p_iX \equiv q_j \bmod m$. Fixem un q_j i el multipliquem a la Identitat de Bézout:

$$amq_j + q_j \sum_{i=1}^{r} p_ia_i = q_j \Longrightarrow amq_j + a_jp_jq_j + \sum_{i=1, i\neq j}^{r} a_ip_iq_j = q_j$$

  Per hipòtesi tenim $p_iq_j \equiv p_jq_i \bmod m$ i ho apliquem a la iqualtat anterior:

$$amq_j + p_j(a_jq_j + \sum_{i=1, i\neq j}^{r} a_iq_i) + ml = q_j$$

Fem mòdul m:

$$p_j(\sum_{i=1,i\neq j}^{r} a_i q_i) \equiv q_j \bmod m$$

Observem que $\sum_{i=1,i\neq j}^{r} a_i q_i$ és el mateix per a $\forall j$, podem concloure que és la B buscada.

□

Lema 1.2.8. *Siguin $f(x,y) = a_1x^2 + b_1xy + c_1y^2$ i $g(x,y) = a_2x^2 + b_2xy + c_2y^2$ dues formes de Dirichlet. Aleshores existeix un únic enter $B \equiv 0$ mod $2a_1a_2$ tal que:*

$$B \equiv b_1 \ mod\ 2a_1$$
$$B \equiv b_2 \ mod\ 2a_2$$
$$B^2 \equiv D \ mod\ 4a_1a_2$$

Demostració. • Si B és un enter que compleix les dues primeres congruències, aleshores:

$$B - b_1 = 2a_1l$$
$$B - b_2 = 2a_2l'$$

Multipliquem aquestes dues igualtats i fem mòdul $4a_1a_2$:

$$(B-b_1)(B-b_2) = B^2 - B(b_1+b_2) + b_1b_2 = 4a_1a_2L \Longrightarrow$$
$$\Longrightarrow (B-b_1)(B-b_2) \equiv B^2 - B(b_1+b_2) + b_1b_2 \equiv 0 \bmod 4a_1a_2$$

Podem escriure $B^2 = B(b_1+b_2) - b_1b_2 - 4a_1a_2L$ i per tant, la tercera congruència:

$$B^2 - D = 4a_1a_2n \Longrightarrow B(b_1+b_2) - (D+b_1b_2) = 4a_1a_2N$$
$$B(b_1+b_2) \equiv D + b_1b_2 \bmod 4a_1a_2 \Longrightarrow B\frac{b_1+b_2}{2} \equiv \frac{D+b_1b_2}{2} \bmod 2a_1a_2$$

Prenem ara les dues primeres congruències i les multipliquem per a_2 i a_1 respectivament. Les congruències del lema són equivalents a:

$$a_2B \equiv a_2b_1 \bmod 2a_1a_2$$
$$a_1B \equiv a_1b_2 \bmod 2a_1a_2$$
$$\frac{b_1+b_2}{2}B \equiv \frac{D+b_1b_2}{2} \bmod 2a_1a_2$$

• Per hipòtesi $mcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$, mirem que aquestes congruències compleixin les del lema anterior per poder aplicar-lo.

És clar que les dues primeres congruències compleixen la hipòtesi $p_iq_j \equiv p_jq_i \mod 2a_1a_2$ del Lema 1.2.7 ja que $p_iq_j = p_jq_i = a_1a_2b_1$.

Ho comprovem per la primera i la tercera:

$$a_2B - a_2b_1 = 2a_1a_2l$$
$$\frac{b_1+b_2}{2}B - \frac{D+b_1b_2}{2} = 2a_1a_2l'$$

multipliquem la primera per $\frac{b_1+b_2}{2}$ i l'altra per a_2 i restem de manera que obtenim $a_2\frac{D+b_1b_2}{2} - a_2b_1\frac{b_1+b_2}{2} = 2a_1a_2L$ i obtenim la congruència buscada.

Seguim el mateix procediment per comprovar-ho amb la segona i tercera congruència i obtenim $a_1\frac{D+b_1b_2}{2} - a_1b_1\frac{b_1+b_2}{2} = 2a_1a_2L'$.

Apliquem el Lema 1.2.7 i comprovem l'existència i unicitat de B mòdul $2a_1a_2$ com volíem.

□

Proposició 1.2.9. *Siguin (a_1, b_1, c_1) i (a_2, b_2, c_2) dues formes de Dirichlet, existeixen enters B i C tals que*

$$(a_1, b_1, c_1) \sim (a_1, B, a_2C)$$

i

$$(a_2, b_2, c_2) \sim (a_2, B, a_1C)$$

Demostració. Sigui $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ una matriu de canvi, si prenem T^n sobre una forma (a, b, c), la forma pròpiament equivalent resultant és $(a, b + 2an, c')$ per algun $c' \in \mathbb{Z}$.

Utilitzem T^n com a matriu de canvi per (a_1, b_1, c_1) i prenem n tal que $b_1 + 2a_1n \equiv b_1 \mod 2a_1$. Alhora, per (a_2, b_2, c_2) prenem T^m com a matriu de canvi on m sigui tal que $b_2 + 2a_2m \equiv b_2 \mod 2a_2$. Pel Lema 3.4 sabem que existeix B tal que $B \equiv b_1 \mod 2a_1$, $B \equiv b_2 \mod 2a_2$ i $B^2 \equiv D \mod 4a_1a_2$.

Prenem $B = b_1 + 2a_1n = b_2 + 2a_2m$. Observem que $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, fent el canvi sobre (a_1, b_1, c_1), obtenim $(a_1, B, a_1n^2 + b_1n + c_1)$. Per la definició de B tenim $n = \frac{B-b_1}{2a_1}$. Substituïm i calculem l'últim paràmetre de la forma equivalent

$$a_1(\frac{B - b_1}{2a_1})^2 + b_1\frac{B - b_1}{2a_1} + c_1 = \frac{B^2 - D}{4a_1} = a_2C$$

on $C = \frac{B^2-D}{4a_1a_2}$. Per (a_2, b_2, c_2) seguim el mateix procediment i obtenim les equivalències pròpies que buscàvem. □

Lema 1.2.10. *Dues formes (a_1, b_1, c_1) i (a_2, b_2, c_2) amb el mateix discriminant són equivalents si i només si existeixen enters α i γ tals que*

$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2 \\ 2a_1\alpha + (b_1 + b_2)\gamma &\equiv 0 \ (mod\ 2a_2) \\ (b_1 - b_2)\alpha + 2c_1\gamma &\equiv 0 \ (mod\ 2a_2) \end{aligned}$$

Demostració. Donades les formes (a_1, b_1, c_1) i (a_2, b_2, c_2), si són equivalents, existeix una matriu $A = \begin{pmatrix} \alpha & \beta \\ \delta & \gamma \end{pmatrix} \in SL_2(\mathbb{Z})$ tal que, com hem vist a l'equació (1.2):

$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2 \\ b_1(\alpha\delta + \beta\gamma) + 2(a_1\alpha\beta + c_1\gamma\delta) &= b_2 \\ a_1\beta^2 + b_1\beta\delta + c_1\delta^2 &= c_2 \end{aligned} \tag{1.6}$$

Amb això tenim comprovada la primera equació.

Reescrivim la segona equació de (1.6) com

$$(b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\beta\gamma)\delta = b_2$$

Volem trobar β i δ de manera que

$$\begin{aligned} \alpha\delta - \beta\gamma &= 1 \\ (b_1\gamma + 2a_1\alpha)\beta + (b_1\alpha + 2c_1\beta\gamma)\delta &= b_2 \end{aligned}$$

Les congruències del lema surten de resoldre per β i δ les següents equacions:

$$\begin{aligned} 2a_1\alpha + (b_1 + b_2)\gamma &= 2a_2\delta \\ (b_1 - b_2)\alpha + 2c_1\gamma &= -2a_2\beta \end{aligned}$$

Per demostrar la implicació contrària cal seguir el mateix procediment però en sentit oposat. □

Lema 1.2.11. *Donades dues formes (a_1, B, a_2C) i (a_2, B, a_1C) que són de Dirichlet i B, C definides a la Proposició 1.2.9, podem escriure la seva composició com*

$$(a_1, B, a_2C) * (a_2, B, a_1C) = (a_1a_2, B, C)$$

amb

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$$

i, en aquest cas, la composició està ben definida.

Demostració. Dividim la demostració en dues parts.

- Definim $\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix} = \begin{pmatrix} xz - Cyw \\ a_1xw + a_2yz + Byw \end{pmatrix}$. Calculem la composició de (a_1, B, a_2C) i (a_2, B, a_1C) per (X, Y) definides.

$$(a_1x^2 + Bxy + a_2Cy^2) * (a_2z^2 + Bzw + a_1Cw^2) =$$

$$= a_1a_2x^2z^2 + a_1Bx^2zw + a_1^2Cx^2w^2 + a_2Bxyz^2 + B^2xyzw + a_1BCxyw^2 +$$

$$+ a_2^2Cy^2z^2 + a_2BCy^2zw + a_1a_2C^2y^2w^2 =$$

$$= a_1a_2(xz - Cyw)^2 + B(xz - Cyw)(a_1xw + a_2yz + Byw) + C(a_1xw + a_2yz + Byw)^2 =$$

$$= a_1a_2X^2 + BXY + CY^2$$

  com voliem comprovar.

- Veiem que està ben definida. Considerem f i g formes de Dirichlet i $f \sim f'$, $g \sim g'$ i volem veure que $f * g \sim f' * g'$. Assumim que tenim

$$\begin{aligned} f &= (a_1, B, a_2C) \\ g &= (a_2, B, a_1C) \\ f' &= (m_1, N, m_2L) \\ g' &= (m_2, N, m_1L) \end{aligned}$$

  Definim les enters x, z, y, w pel Lema 1.2.10 tals que

$$\begin{aligned} a_1x^2 + Bxy + a_2Cy^2 &= m_1 \\ 2a_1x + (B + N)y &\equiv 0 \pmod{2m_1} \\ (B - N)x + 2a_2Cy &\equiv 0 \pmod{2m_1} \end{aligned} \tag{1.7}$$

$$\begin{aligned} a_2z^2 + Bzw + a_1Cw^2 &= m_2 \\ 2a_2z + (B + N)w &\equiv 0 \pmod{2m_2} \\ (B - N)z + 2a_2Cw &\equiv 0 \pmod{2m_2} \end{aligned} \tag{1.8}$$

Volem veure que existeixen enters X, Y tals que

$$\begin{aligned} a_1a_2X^2 + BXY + CY^2 &= m_1m_2 \\ 2a_1a_2X + (B+N)Y &\equiv 0 \pmod{2m_1m_2} \\ (B-N)X + 2CY &\equiv 0 \pmod{2m_1m_2} \end{aligned} \tag{1.9}$$

Si definim X i Y com a l'apartat anterior i multipliquem les dues primeres equacions de (1.7) i (1.8), obtenim la primera equació de (1.9).

Sabem que f i f' tenen el mateix discriminant, per tant $N^2 = B^2 - 4a_1a_2C + 4m_1m_2C$. Prenent les primeres congruències de (1.7) i (1.8) i amb la observació feta, trobem

$$(a_1x + \frac{(B+N)y}{2})(a_2z + \frac{(B+N)w}{2}) \equiv a_1a_2X + \frac{(B+N)Y}{2} \pmod{m_1m_2}$$

Queda demostrada així la primera congruència de (1.9). Per demostrar la segona congruència, observem que escrivint

$$\frac{(B-\sqrt{D})X}{2} + CY = U$$

on D és el discriminant de les formes considerades, les següents quatre equacions són immediates:

$$\begin{aligned} (\frac{(B-\sqrt{D})x}{2} + a_2Cy)(a_2z + \frac{(B+\sqrt{D})w}{2}) &= a_2U \\ (a_1x + (B+\sqrt{D})y)(\frac{(B-\sqrt{D})z}{2} + a_1Cw) &= a_1U \\ (\frac{(B-\sqrt{D})x}{2} + a_2Cy)(\frac{(B-\sqrt{D})z}{2} + a_1Cw) &= \frac{(B-\sqrt{D})U}{2} \\ C(a_1x + (B+\sqrt{D})y)(a_2z + (B+\sqrt{D})w) &= \frac{(B+\sqrt{D})U}{2} \end{aligned}$$

Podem substituir N per $\sqrt{D}$ i convertint aquestes quatre equacions en congruències mòdul m_1m_2. Com que la part esquerra de les equacions és congruent a 0 mòdul m_1m_2 i les formes són de Dirichlet, tenim $U \equiv 0 \pmod{m_1m_2}$, que és el que busquem a la segona congruència de (1.9).

□

Corol·lari 1.2.12. *Si (a_1, b_1, c_1) i (a_2, b_2, c_2) són formes de Dirichlet, aleshores a $C(D)$, el conjunt de classes de formes primitives definides positives de discriminant D,*

$$[a_1, b_1, c_1] * [a_2, b_2, c_2] = [a_1a_2, B, C]$$

on $*$ s'anomena la composició de Dirichlet.

Demostració. Per la Proposició 1.2.9 tenim $(a_1, b_1, c_1) \sim (a_1, B, a_2C)$ i $(a_2, b_2, c_2) \sim (a_2, B, a_1C)$. Pel Lema 1.2.11 $(a_1, B, a_2C) * (a_2, B, a_1C) = (a_1a_2, B, C)$ amb

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} xz \\ xw \\ yz \\ yw \end{pmatrix}$$

Tenim

$$(a_1, b_1, c_1) \sim (a_1, B, a_2C)$$
$$(a_2, b_2, c_2) \sim (a_2, B, a_1C)$$
$$(a_1, B, a_2C) * (a_2, B, a_1C) = (a_1a_2, B, C)$$

Anteriorment hem vist que la composició està ben definida per equivalències pròpies entre formes de Dirichlet, per tant:

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) \sim (a_1, B, a_2C) * (a_2, B, a_1C) = (a_1a_2, B, C)$$

a $C(D)$ i fent classes, obtenim $[a_1, b_1, c_1] * [a_2, b_2, c_2] = [a_1a_2, B, C]$

□

Definició 1.2.2. Siguin $f(x, y) = a_1x^2 + b_1xy + c_1y^2$ i $g(x, y) = a_2x^2 + b_2xy + c_2y^2$ formes de Dirichlet de discriminant $D < 0$. Aleshores la *composició de Dirichlet* de $f(x, y)$ i $g(x, y)$ és la forma

$$F(x, y) = a_1a_1x^2 + Bxy + \frac{B^2 - D}{4a_1a_1}y^2$$

on B és l'enter determinat pel Lema 1.2.8.

Ara ja estem en condicions de donar el resultat principal d'aquesta secció.

Teorema 1.2.13. *Sigui $D \equiv 0, 1 \ mod\ 4$ un enter negatiu. Aleshores, la composició de Dirichlet indueix una operació binària ben definida sobre $C(D)$ que fa $C(D)$ un grup Abelià finit d'ordre $h(D)$. A més, l'element identitat de $C(D)$ és la classe que contingui la forma*

$$x^2 - \frac{D}{4}y^2 \ \textit{si}\ D \equiv 0 \ mod\ 4$$
$$x^2 + xy + \frac{1 - D}{4}y^2 \ \textit{si}\ D \equiv 1 \ mod\ 4,$$

i l'invers de la classe de $ax^2 + bxy + cy^2$ és la classe que conté $ax^2 - bxy + cy^2$.

Observació 1.5.

- *El conjunt $C(D)$ amb la composició de Dirichlet s'anomena* ***grup de classes****.*
- *La forma $ax^2 - bxy + cy^2$ s'anomena forma* ***oposada*** *de $ax^2 + bxy + cy^2$.*

Demostració. Prèviament hem vist que la composició per a formes de Dirichlet està ben definida. Ens cal veure que és una operació commutativa, associativa, amb element neutre i invers.

- Commutativitat: Tenim $[a_1, b_1, c_1] * [a_2, b_2, c_2] = [a_1a_2, B, C]$ amb

$$B \equiv b_1 \mod 2a_1$$
$$B \equiv b_2 \mod 2a_2$$
$$B^2 \equiv D \mod 4a_1a_2$$
$$C = \frac{B^2 - D}{4a_1a_2}$$

Alhora $[a_2, b_2, c_2] * [a_1, b_1, c_1] = [a_1a_2, B', C']$ i

$$B' \equiv b_1 \mod 2a_1$$
$$B' \equiv b_2 \mod 2a_2$$
$$B'^2 \equiv D \mod 4a_1a_2$$
$$C' = \frac{B'^2 - D}{4a_1a_2}$$

Per les congruències tenim $B = B'$ i, en conseqüència, $C = C'$ i $[a_1, b_1, c_1] * [a_2, b_2, c_2] = [a_2, b_2, c_2] * [a_1, b_1, c_1]$.

- Associativitat: Per un costat tenim $[a_1, b_1, c_1]*([a_2, b_2, c_2]*[a_3, b_3, c_3]) = [a_1, b_1, c_1]*[a_2a_3,^1 B,^1 C] = [a_1a_2a_3, B, C]$ i per tant

$$\begin{aligned} {}^1B &\equiv b_2 \mod 2a_2 \\ {}^1B &\equiv b_3 \mod 2a_3 \\ ({}^1B)^2 &\equiv D \mod 4a_2a_3 \\ B &\equiv b_1 \mod 2a_1 \\ B &\equiv ({}^1B) \mod 2a_2a_3 \\ B^2 &\equiv D \mod 4a_1a_2a_3 \end{aligned} \tag{1.10}$$

Si prenem $B_k = B+4a_1a_2a_3k$, compleix totes les congruències de (7). Per l'altre costat tenim $([a_1, b_1, c_1] * [a_2, b_2, c_2]) * [a_3, b_3, c_3]) = [a_1a_2,^2 B,^2 C] * [a_3, b_3, c_3] = [a_1a_2a_3, B', C']$ i

$$\begin{aligned} {}^2B &\equiv b_1 \mod 2a_1 \\ {}^2B &\equiv b_2 \mod 2a_2 \\ ({}^2B)^2 &\equiv D \mod 4a_1a_2 \\ B' &\equiv ({}^2B) \mod 2a_1a_2 \\ B' &\equiv b_3 \mod 2a_3 \\ (B')^2 &\equiv D \mod 4a_1a_2a_3 \end{aligned} \tag{1.11}$$

Volem comprovar que B_k compleix (1.11).

És clar que l'última congruència de (1.10) implica que B_k compleix l'última de (1.11).

Observem que $B_k \equiv B \equiv ({}^1B) \equiv b_3 \mod 2a_3$ i prenent $B_k \equiv ({}^2B_k) \mod 2a_1$ i $B_k \equiv ({}^2B_k) \mod 2a_2$

$$\begin{aligned} B_k \equiv B \equiv b_1 \mod 2a_1 \\ B_k \equiv B \equiv ({}^1B) \equiv b_2 \mod 2a_2 \end{aligned}$$

aquestes congruències impliquen $B_k \equiv ({}^2B_k) \mod 2a_1a_2 \Longrightarrow B_k = ({}^2B_k) + 2a_1a_2k'$. Alhora tenim $D \equiv B^2 \equiv (B_k)^2 \equiv ({}^2B_k)^2 \mod 4a_1a_2$.

B_k compleix (1.10) i (1.11), per tant $B_k \equiv B \equiv B' \mod 4a_1a_2a_3$, en conseqüència, $C \equiv C'$, tenim associativitat.

- Identitat:

1. Considerem $D \equiv 0 \mod 4$ i prenem (a, b, c) de discriminant D. Per $D \equiv 0 \mod 4$ sabem que b és parell. Fem $[a, b, c] * [1, 0, -\frac{D}{4}] = [a, B, C]$. B ha de complir

$$\begin{aligned} B &\equiv b \mod 2a \\ B &\equiv 0 \mod 2 \\ B^2 &\equiv D \mod 4a. \end{aligned}$$

   Prenent $B = b$ es compleixen aquestes congruències, a més $C = \frac{B^2-D}{4a} = \frac{b^2-(b^2-4ac)}{4a} = c$. Per tant, $[a, b, c] * [1, 0, -\frac{D}{4}] = [a, b, c]$ i $[1, 0, -\frac{D}{4}] * [a, b, c] = [a, b, c]$ per commutativitat.

2. Considerem ara $D \equiv 1 \mod 4$ i (a, b, c) de discriminant D; en aquest cas b és senar. Fem $[a, b, c] * [1, 1, \frac{1-D}{4}] = [a, B, C]$; com al cas anterior, prenent $B = b$ es compleixen les congruències del lema 1.2.7 i $C = c$.

Hem comprovat que l'element identitat és $[1, 0, \frac{D}{4}]$ si $D \equiv 0 \mod 4$ i $[1, 1, \frac{1-D}{4}]$ si $D \equiv 1 \mod 4$.

- Invers: Per últim comprovarem que l'element invers de $[a, b, c]$ és la classe que conté $[a, -b, c]$. Observem que $[a, b, c]$ i $[a, -b, c]$ no són formes de Dirichlet ja que $mcd(a, a, \frac{b-b}{2}) = a > 1$ i no podem fer la seva composició de Dirichlet directament.

  Prenent $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ i aplicant el canvi a $(a, -b, c)$, tenim $(a, -b, c) \sim (c, b, a)$ i, en conseqüència $[a, -b, c] = [c, b, a]$. Amb aquesta equivalència $[a, b, c]$ i $[c, b, a]$ sí que són formes de Dirichlet i podem fer-ne la composició de Dirichlet. $[a, b, c] * [c, b, a] = [ac, B, C]$ on

$$\begin{aligned} B &\equiv b \mod 2a \\ B &\equiv b \mod 2c \\ B^2 &\equiv D \mod 4ac. \end{aligned}$$

  Prenent $B = b$ es compleixen les congruències i $C = 1$. Hem vist $[a, b, c] * [c, b, a] = [ac, b, 1]$, ara cal comprovar que $(ac, b, 1) \sim 1_D$, on 1_D és la identitat. Amb el canvi $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ tenim $(ac, b, 1) \sim (1, -b, ac)$ i amb $T^n = (\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})^n$, $(1, -b, ac) \sim (1, -b + 2n, c')$. Si $D \equiv 0 \mod 4$, b és parell i prenem n tal que $-b + 2n = 0$. Com es veu a la demostració de la Proposició 1.2.9, $c' = n^2 - bn + ac = (\frac{b}{2})^2 - b\frac{b}{2} + ac = -\frac{D}{4}$. Per tant, $[a, b, c] * [c, b, a] = [ac, b, 1] = [1, 0, -\frac{D}{4}]$. Si $D \equiv 1 \mod 4$, b és senar i prenem n tal que $-b + 2n = 1$, aleshores tenim $c' = n^2 - bn + ac = \frac{1-D}{4}$ i, en conseqüència, $[a, b, c] * [c, b, a] = [ac, b, 1] = [1, 1, \frac{1-D}{4}]$.

Hem comprovat que $C(D)$ amb la composició de Dirichlet és un grup abelià finit (tot explicitant identitat 1_D i invers).

□

Exemple 1.2.14. *Veiem un exemple on es comproven aquestes propietats. Prenem* $f(x, y) = (3, 3, 4)$, $g(x, y) = (2, 1, 5)$ *i* $h(x, y) = (2, -3, 6)$, *que son formes de* $C(-39)$. *Per fer els càlculs utilitzem el programa de SageMath que es troba a l'Apèndix B.*

- *Commutativitat:*

$$\begin{aligned} [3, 3, 4] * [2, 1, 5] &= [6, 3, 2] = [2, -1, 5] \\ [2, 1, 5] * [3, 3, 4] &= [6, 3, 2] = [2, -1, 5] \end{aligned}$$

- *Associativitat:*

$$\begin{aligned} [3, 3, 4] * ([2, 1, 5] * [2, -3, 6]) &= [3, 3, 4] * [12, 3, 1] = [3, 3, 4] \\ ([3, 3, 4] * [2, 1, 5]) * [2, -3, 6] &= [6, 3, 2] * [2, -3, 6] = [4, 3, 3] = [3, 3, 4] \end{aligned}$$

- *Identitat:* $f, g, h \in C(-39)$, *per tant* $1_D = [1, 1, 10]$.

$$\begin{aligned} [3, 3, 4] * [1, 1, 10] &= [3, 3, 4] \\ [1, 1, 10] * [3, 3, 4] &= [3, 3, 4] \end{aligned}$$

- *Invers:*

$$\begin{aligned} [3, 3, 4] * [3, -3, 4] &= [12, 3, 1] = [1, 1, 10] \\ [3, -3, 4] * [3, 3, 4] &= [12, 3, 1] = [1, 1, 10] \end{aligned}$$

- *Calculem ara l'ordre dels elements de $C(-39)$. Es poden trobar llistats a la Taula C.1.*

$$[2,1,5]*[2,1,5]=[3,3,4],\ [3,3,4]*[2,1,5]=[2,-1,5]\ i\ [2,-1,5]*[2,1,5]=[1,1,10]$$
$$[2,-1,5]*[2,-1,5]=[3,3,4],\ [3,3,4]*[2,-1,5]=[2,1,5],\ [2,1,5]*[2,-1,5]=[1,1,10]$$
$$[3,3,4]*[3,3,4]=[1,1,10]$$

  Per tant, $O([3,3,4])=2$ i $O([2,1,5])=O([2,-1,5])=4$, fet que ens permet dir que $C(-39)\cong\mathbb{Z}/(4)$.

Si ara prenem $C(-87)$, que és un grup de 6 elements, i calculem els seus ordres:

$$[2,1,11]^6=[1,1,22]$$
$$[2,-1,11]^6=[1,1,22]$$
$$[3,3,8]^2=[1,1,22]$$
$$[4,3,6]^3=[1,1,22]$$
$$[4,-3,6]^3=[1,1,22]$$

Observem que, en aquest cas, $C(-87)\cong\mathbb{Z}/(6)\cong\mathbb{Z}/(2)\times\mathbb{Z}/(3)$.

A *Disquisitiones Arithmeticae* [7] Gauss fa una conjectura dient que per a discriminants $D<0$, tenim $h(D)\longrightarrow\infty$ quan $D\longrightarrow-\infty$. Heilbronn (1934) i Siegel (1936) demostren que per a qualsevol $\epsilon>0$, existeix una constant $c_\epsilon>0$ tal que per a $|D|$

$$h(D)\geq c_\epsilon|D|^{\frac{1}{2}-\epsilon}$$

Seigel demostra aquest fet assumint la Hipòtesi generalitzada de Riemann, però això ofereix una prova no efectiva per a determinar els valors d'una m donada per a una llista completa de discriminants $D<0$ tal que $h(D)=m$. Aquest problema és conegut com a *problema de nombres de classes de Gauss*. Goldfeld (1976) i Gross i Zagier (1983) demostren que, donades certes condicions tècniques, per a qualsevol $\epsilon>0$, existeix una constant efectiva i computable c_ϵ tal que:

$$h(D)>c_\epsilon ln(|D|)^{1-\epsilon}$$

De manera que aconseguim una fita inferior per a $h(D)$. Podeu consultar les referències per a més detalls sobre les demostracions de Heilbronn [10], Goldfeld, Gross i Zagier [8], [9].

1.3 Ideals en cossos quadràtics

Dirichlet també utilitza la notació d'ideals en cossos quadràtics imaginaris per descriure la composició de formes de Dirichlet.

Definició 1.3.1. Diem que el complex α és un *nombre algebraic quadràtic* si satisfà l'equació polinomial

$$ax^2+bx+c=0$$

on $a,b,c\in\mathbb{Z}$ amb $ac\neq0$.

Un nombre algebraic quadràtic és un *enter algebraic quadràtic* si satisfà l'equació polinomial

$$x^2+bx+c=0$$

on $b,c\in\mathbb{Z}$, $c\neq0$.

Els nombres algebraics quadràtics són, precisament, els complexos de la forma

$$\frac{-b+e\sqrt{d}}{2a}$$

on $a, b, d, e \in \mathbb{Z}$ amb $d \neq 0$ lliure de quadrats.

Diem que d és el *radical* del nombre algebraic quadràtic α.

Sabem de teoria de cossos que per α un nombre algebraic de radical d, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$ i una $\mathbb{Q}$-base és $(1, \sqrt{d})$.

Definició 1.3.2. Sigui $d \neq 1$ un enter lliure de quadrats, definim Δ com:

- $\Delta = 4d$ si $d \equiv 2, 3 \mod 4$
- $\Delta = d$ si $d \equiv 1 \mod 4$

Ara, amb d i Δ definits, podem anomenar a $\mathbb{Q}(\sqrt{d})$ el *cos de nombres quadràtics* de radical d i discriminant Δ. Observem que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$.

Proposició 1.3.1. *Sigui $d \neq 1$ un enter lliure de quadrats. El conjunt d'enters algebraics quadràtics de radical d és:*

- $\{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$, *si* $d \equiv 2, 3 \mod 4$
- $\{(a + b\sqrt{d})/2 : a, b \in \mathbb{Z}, a \equiv b \mod 2\}$, *si* $d \equiv 1 \mod 4$

Aquest conjunt és un domini sota la suma i multiplicació dins el cos $\mathbb{Q}(\sqrt{d})$.

Demostració. Considerant les definicions prèvies, α és un enter algebraic quadràtic si és de la forma $\frac{-b+e\sqrt{d}}{2}$ on $b^2 - 4c = e^2 d$. Considerant aquesta última equació mòdul 4, tenim, per $d \equiv 2, 3 \mod 4$, que b i e han de ser enters parells. Si $d \equiv 1 \mod 4$, b i e han de tenir la mateixa paritat.

Per veure que és un domini, només cal veure que la suma i la multiplicació són tancades en aquests conjunts i és clar per definició.

□

Al domini definit a la Proposició 1.3.1, l'anomenem *anell d'enters* de $\mathbb{Q}(\sqrt{d})$ i l'escrivim $\mathcal{O}(\sqrt{d})$.

Per conveniència, posem δ que sigui $-\sqrt{d}$ o $(1-\sqrt{d})/2$ segons si el discriminant del cos és parell o senar. Amb aquesta notació, podem escriure $\mathcal{O}(\sqrt{d})$ com $\{a + b\delta : a, b \in \mathbb{Z}\}$.

Definició 1.3.3. Per a qualsevol nombre algebraic quadràtic $\alpha = \frac{-b+e\sqrt{d}}{2a}$, el *conjugat* de α és $\overline{\alpha} = \frac{-b-e\sqrt{d}}{2a}$.

La *norma* de α és $N(\alpha) = \alpha\overline{\alpha} = \frac{b^2+e^2 d}{4a^2}$. La norma d'un enter algebraic quadràtic és sempre un enter i és una funció multiplicativa, és a dir, per a qualssevol enters α i β, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Un element ϵ de $\mathcal{O}(\sqrt{d})$ és una *unitat* de l'anell si té norma ± 1.

Lema 1.3.2. *Sigui $\mathcal{U}$ un ideal de l'anell d'enters $\mathcal{O}(\sqrt{d})$, aleshores existeixen $\alpha_1, \alpha_2 \in \mathcal{U}$ tals que qualsevol element de $\mathcal{U}$ s'escriu com $\alpha_1 x + \alpha_2 y$, amb $x, y \in \mathbb{Z}$.*

Demostració. Observem que $\mathcal{U} \leq \mathcal{O}(\sqrt{d})$ és un subgrup d'un DIP com a $\mathbb{Z}$-mòdul lliure de rang 2. Per la classificació de DIPs lliures tenim $\mathcal{U} \cong (\mathbb{Z}, +)$ o bé $\mathcal{U} \cong (\mathbb{Z}^2, +)$; la primera opció no és possible ja que $\mathcal{U}$ és un $\mathcal{O}(\sqrt{d})$-mòdul i hauriem de tenir $a\mathbb{Z}$ o $a\sqrt{D}\mathbb{Z}$ però a i $\sqrt{D}$ són linealment independents a $\mathbb{Q}(\sqrt{D})$. Per tant, $\mathcal{U} \cong (\mathbb{Z}^2, +)$ i queda demostrat el lema.

□

La parella $< \alpha_1, \alpha_2 >$, s'anomena *base* de l'ideal $\mathcal{U}$, normalment escriurem $\mathcal{U} =< \alpha_1, \alpha_2 >$.

Proposició 1.3.3. *Qualsevol ideal $\mathcal{U}$ té una base $< a, b+g\delta >$, on $a, b, g \in \mathbb{Z}$ amb $a > 0, 0 \leq b < a$, i $0 < g \leq a$, i g divideix a i b. La $\mathbb{Z}$-base de $\mathcal{U}$ amb aquestes propietats és única.*

Demostrarem aquesta proposició a partir dels lemes següents.

Lema 1.3.4. *Qualsevol ideal $\mathcal{U}$ té una base $< a, \beta >$, on a és un enter i β un enter algebraic quadràtic.*

Demostració. Els elements de $\mathcal{O}(\sqrt{d})$ són de la forma $a + b\delta$, per $a, b \in \mathbb{Z}$. Això ha de ser cert per als elements de la base, per tant podem escriure $\alpha_1 = a_1 + b_2\delta$ i $\alpha_2 = a_2 + b_2\delta$ amb $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Com que $\alpha_1 x + \alpha_2 y = \alpha_1(x + ky) + (\alpha_2 - k\alpha_1)y$ per a qualsevol enter k, tenim $< \alpha_1, \alpha_2 - k\alpha_1 >$, i per simetria $< \alpha_1 - k\alpha_2, \alpha_2 >$, és una $\mathbb{Z}$-base equivalent per a $\mathcal{U}$. Utilitzant l'algorisme d'Euclides sobre b_1 i b_2 trobem una base $< a, b + g\delta >$ d'$\mathcal{U}$ amb enters a, b, g que és equivalent a la base $< \alpha_1, \alpha_2 >$ i on $0 \neq g = \text{mcd}(b_1, b_2)$. Caldrà fer un pas més treient múltiples de a i b per poder assumir $0 \leq b < a$.

□

Lema 1.3.5. *Un ideal $\mathcal{U}$ té una única base de la forma $< a, b + g\delta >$, amb $a, b, g \in \mathbb{Z}$, $a > 0$, $0 \leq b < a$, i $0 < g \leq a$; aquesta base s'anomena base canònica, també podem escriure $(a, b + g\delta)_{\mathcal{O}(\sqrt{\Delta})}$ ja que $\mathcal{U}$ és un ideal de $\mathcal{O}(\sqrt{\Delta})$.*

Demostració. Donada qualsevol base de $\mathcal{U}$, per la Proposició 1.3.3, tenim una base equivalent de la forma $< a, b + g\delta >$ amb $a, b, g \in \mathbb{Z}$ i a i b complint les condicions desitjades.

Observem que pel Lema 1.3.2, qualsevol enter m que pertany a $\mathcal{U}$ té una representació única i la representació amb la base de la Proposició 1.3.4, $m = ax + (b + g\delta)y$, també ha de ser única. Per tant, $y = 0$. En conseqüència, qualsevol enter de $\mathcal{U}$ és un múltiple de a.

Vist això, l'enter a de la base està únicament determinat per l'ideal. Si tenim dues bases diferents $< a, b + g\delta >$ i $< a, b' + g'\delta >$, podem trobar dos enters x i y tals que $ax + (b + g\delta)y = b' + g'\delta$. Això implica $ax + by = b'$ i $gy = g'$. Si b i b' estan entre 0 i a, implica que $x = 0$ i $y = 1$, per tant, tenim que g és únic. g ha de complir $0 < g \leq a$; tenim $a, a\delta \in \mathcal{U}$ i per tant, hi ha una única representació per $a\delta = ax + (b + g\delta)y \Longrightarrow gy = a \Longrightarrow 0 < g \leq a$.

□

Definició 1.3.4. Donat un ideal $\mathcal{U} =< \alpha_1, \alpha_2 >$, definim la *norma* de $\mathcal{U}$ és $N(\mathcal{U}) = \frac{|\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2|}{\sqrt{\Delta}}$, on Δ és el discriminant del cos de radical d.

Lema 1.3.6. *La norma $N(\mathcal{U})$ d'un ideal $\mathcal{U}$ no depen de la $\mathbb{Z}$-base triada.*

Demostració. Prenem $B =< \alpha_1, \alpha_2 >$ una $\mathbb{Z}$-base de $\mathcal{U}$, tenim:

$$N(\mathcal{U}) = \frac{|\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2|}{\sqrt{\Delta}}$$

Considerem ara $B' =< A\begin{pmatrix}1\\0\end{pmatrix}_B, A\begin{pmatrix}0\\1\end{pmatrix}_B >_{\mathbb{Z}} =< n_1\alpha_1 + n_2\alpha_2, q_1\alpha_1 + q_2\alpha_2 >$ on $A = \begin{pmatrix}n_1 & q_1\\ n_2 & q_2\end{pmatrix} \in SL_2(\mathbb{Z})$, $n_1q_2 - n_2q_1 = 1$. Amb B' calculem la norma de $\mathcal{U}$:

$$N(\mathcal{U}) = \frac{|(n_1\alpha_1 + n_2\alpha_2)(\overline{q_1\alpha_1 + q_2\alpha_2}) - (\overline{n_1\alpha_1 + n_2\alpha_2})(q_1\alpha_1 + q_2\alpha_2)|}{\sqrt{\Delta}} =$$

$$\frac{|(n_1\alpha_1 + n_2\alpha_2)(q_1\overline{\alpha_1} + q_2\overline{\alpha_2}) - (n_1\overline{\alpha_1} + n_2\overline{\alpha_2})(q_1\alpha_1 + q_2\alpha_2)|}{\sqrt{\Delta}} =$$

$$= \frac{|n_1q_2\alpha_1\overline{\alpha_2} + n_2q_1\overline{\alpha_1}\alpha_2 - n_1q_2\overline{\alpha_1}\alpha_2 - n_2q_1\alpha_1\overline{\alpha_2}|}{\sqrt{\Delta}} =$$
$$= \frac{|(n_1q_2 - n_2q_1)(\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2)|}{\sqrt{\Delta}} = \frac{|\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2|}{\sqrt{\Delta}}$$

□

Definició 1.3.5. Un *ideal fraccional* és un subconjunt $\mathcal{I}$ de $\mathbb{Q}(\sqrt{\Delta})$ on es compleixen les següents propietats:

- per a qualssevol $\alpha, \beta \in \mathcal{I}$ i $\lambda, \mu \in \mathcal{O}(\sqrt{\Delta})$, $\lambda\alpha + \mu\beta \in \mathcal{I}$.
- existeix un enter algebraic fixat v tal que, per a qualsevol $\alpha \in \mathcal{I}$, $v\alpha \in \mathcal{O}(\sqrt{\Delta})$.

Notem que qualsevol ideal de $\mathcal{O}(\sqrt{\Delta})$ és un ideal fraccional. Si prenem v com a la definició, aleshores el conjunt $\{v\alpha : \alpha \in \mathcal{I}\}$ és un ideal de $\mathcal{O}(\sqrt{\Delta})$ amb base canònica $(a, b + g\delta)$, per tant $\mathcal{I}$ té base $(a/v, (b + g\delta)/v)$. Prenem $\Delta < 0$ i observem que en aquest cas, $N(\mathcal{U}) > 0$.

Diem que dos ideals $\mathcal{U}$ i $\mathcal{V}$ són *equivalents* si existeix un ideal principal (α) tal que $\mathcal{U} = (\alpha)\mathcal{V}$. A més, la norma de α és positiva.

Observació 1.6.

- *Donats dos ideals fraccionals, definim el seu producte com:*

$$\mathcal{U}\mathcal{V} = \{\sum_{i=1}^{n} \alpha_i\beta_i | \alpha \in \mathcal{U}, \beta \in \mathcal{V}\}$$

- *Sigui $\mathcal{U}$ un ideal fraccional, escollim $n \in \mathbb{Z} \setminus \{0\}$ tal que $n\mathcal{U} = \mathcal{V}$, aleshores $\mathcal{V}\overline{\mathcal{V}} = (m)$ per algun $m \in \mathbb{Z} \setminus \{0\}$ i tenim*

$$\mathcal{U}(\frac{n}{m}\overline{\mathcal{V}}) = (n\mathcal{U})(\frac{1}{m}\overline{\mathcal{V}}) = \frac{1}{m}(\mathcal{V}\overline{\mathcal{V}}) = \frac{1}{m}(m) = (1)$$

per tant $\mathcal{U}^{-1} = \frac{n}{m}\overline{\mathcal{V}}$

Teorema 1.3.7. *Les classes d'equivalència d'ideals fraccionals de l'anell $\mathcal{O}(\sqrt{\Delta})$ formen un grup abelià sota la multiplicació d'ideals. La identitat del grup és la classe de tots els ideals principals ($N(\alpha) > 0$).*

Demostració. A l'observació anterior hem vist que la multiplicació és associativa i commutativa i que els inversos existeixen, en conseqüència, queda demostrat el Teorema.

□

El grup de classes d'ideals s'anomena *grup de classes.*

Observació 1.7. *Escrivim explícitament el procediment per passar d'ideals a formes binàries i viceversa.*

- *Donat un ideal $\mathcal{U}$ amb base $< \alpha_1, \alpha_2 >$ tal que $\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2 = N(\mathcal{U})\sqrt{\Delta}$ és positiu. La forma binària associada a $\mathcal{U}$ és*

$$\frac{[\alpha_1 x + \alpha_2 y][\overline{\alpha_1}x + \overline{\alpha_2}y]}{|N(\mathcal{U})|}$$

- *Donada una forma binària (A, B, C) de discriminant $\Delta < 0$, podem associar-li l'ideal de base $(A, b + \delta)_{\mathcal{O}(\sqrt{\Delta})}$ on $b = \frac{B}{2}$ si B és parell o bé $b = \frac{B-1}{2}$ si B és senar.*

Teorema 1.3.8. *El grup de classes de formes binàries quadràtiques de discriminant $\Delta < 0$ ($\Delta = D$ amb la notació utilitzada anteriorment) és bijectiu al grup de classes del cos quadràtic $\mathbb{Q}(\sqrt{\Delta})$.*

Demostració. Volem veure que qualsevol ideal correspon a una forma i que qualsevol forma correspon a un ideal, i que ideals equivalents corresponen a formes equivalents, i viceversa.

- Sigui $\mathcal{U}$ un ideal de base $< \alpha_1, \alpha_2 >$. Prenem la base de manera que $\alpha_1\overline{\alpha_2} - \overline{\alpha_1}\alpha_2 = N(\mathcal{U})\sqrt{\Delta}$ és positiu o té part imaginària positiva. La forma binària quadràtica de discriminant Δ que associem amb aquest ideal és

$$\frac{[\alpha_1 x + \alpha_2 y][\overline{\alpha_1}x + \overline{\alpha_2}y]}{|N(\mathcal{U})|} = \frac{1}{|N(\mathcal{U})|}(|\alpha_1|^2x^2 + (\alpha_1\overline{\alpha_2} + \overline{\alpha_1}\alpha_2)xy + |\alpha_2|^2y^2)$$

  Aquesta és una forma binària quadràtica de coeficients enters i discriminant Δ. Com que $\Delta < 0$, és una forma definida positiva; diem que la forma *pertany* a $\mathcal{U}$.

- Per altra banda, sigui (A, B, C) una forma binària quadràtica de discriminant Δ, associem l'ideal

$$\{A\alpha + (b + \delta)\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  on b és $B/2$ o $(B-1)/2$ segons Δ sigui parell o senar. Afegint o treient enters múltiples de A a b, podem fer un ideal idèntic

$$\{A\alpha + (b' + \delta)\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  amb $0 \leq b' < A$. Per tant, $(A, b' + \delta)$ és una base canònica de l'ideal. L'ideal associat a la forma binària quadràtica (A, B, C) té base $(A, b + \delta)$. L norma d'aquest ideal és positiva o té part real positiva i la forma que pertany a aquest ideal és (A, B, C).

- Per veure que formes equivalents pertanyen a ideals equivalents i viceversa, només ens cal veure que això és cert per les matrius $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ i $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, recordem que S i T són els generadors de $SL_2(\mathbb{Z})$ i generen totes les equivalències pròpies de les formes binàries. Per a T ja ho hem vist afegint o treient múltiples de A a b. La matriu S produeix l'equivalència de formes $(A, B, C) \sim (C, -B, A)$, aquesta correspon a l'equivalència dels ideals

$$\{A\alpha + (b + \delta)\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  i

$$\{A(b + \overline{\delta})\alpha + (b + \delta)(b + \overline{\delta})\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  Treiem l'ideal principal (A) per obtenir l'ideal equivalent

$$\{(b + \overline{\delta})\alpha + C\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  i aquest és equivalent a

$$\{C\alpha - (b' + \delta)\beta : \alpha, \beta \in \mathcal{O}(\sqrt{\Delta})\}$$

  Com que C és positiu, ja que la forma és definida positiva, aquest ideal està associat a la forma $(C, B', *)$ equivalent sota transformació de matrius T^n per a cert n, a $(C, -B, A)$.

□

Observació 1.8. *La bijecció correspon a un morfisme de grups.*

Pensem el cas $b = \frac{B}{2}$ *on* Δ *parell fixat.*

Tenim

$$(A_1, B_1, C_1) * (A_2, B_2, C_2) = (A_1A_2, \tilde{B}, \tilde{C})$$

on $\tilde{B}$ *segons el Lema 1.2.8.*

Per altra banda posem $b_1 = \frac{B_1}{2}$, $b_2 = \frac{B_2}{2}$ *i fem*

$$(\alpha A_1 + \beta(b_1 + \delta))(\alpha' A_2 + \beta'(b_2 + \delta)) =$$

$$= \alpha\alpha' A_1A_2 + (\alpha\beta' A_1 + \alpha'\beta A_2 + \beta\beta'(b_1 + b_2 + \delta))\delta + (\alpha\beta' A_1 b_2 + \alpha'\beta A_2 b_1 + \beta\beta' b_1 b_2)$$

Podem trobar $\tilde{B}$ *que compleix les congruències del Lema 1.2.8 i* $\tilde{b} = \frac{\tilde{B}}{2}$ *de manera que*

$$(\alpha A_1 + \beta(b_1 + \delta))(\alpha' A_2 + \beta'(b_2 + \delta)) = \tilde{\alpha} A_1A_2 + \tilde{\beta}(\delta + \tilde{b})$$

Concloent així que el producte de formes va al producte d'ideals.

Exemple 1.3.9. *Considerem* $C(-39)$ *on les formes reduïdes són:* $f_1 = (1, 1, 10)$, $f_2 = (2, 1, 5)$, $f_3 = (2, -1, 5)$ *i* $f_4 = (3, 3, 4)$. *Per a* $\Delta = -39$ *tenim* $\delta = \frac{1-\sqrt{-39}}{2}$ *i seguint el procediment de la demostració i l'observació, podem trobar els ideals associats a les formes reduïdes de* $C(-39)$*:*

- $\mathcal{U}_{f_1} =< 1, \frac{1-\sqrt{-39}}{2} >= \{\alpha + \frac{1-\sqrt{-39}}{2}\beta : \alpha, \beta \in \mathcal{O}(\sqrt{-39})\}$
- $\mathcal{U}_{f_2} =< 2, \frac{1-\sqrt{-39}}{2} >= \{2\alpha + \frac{1-\sqrt{-39}}{2}\beta : \alpha, \beta \in \mathcal{O}(\sqrt{-39})\}$
- $\mathcal{U}_{f_3} =< 2, \frac{-1-\sqrt{-39}}{2} >= \{2\alpha + \frac{-1-\sqrt{-39}}{2}\beta : \alpha, \beta \in \mathcal{O}(\sqrt{-39})\}$
- $\mathcal{U}_{f_4} =< 3, \frac{3-\sqrt{-39}}{2} >= \{3\alpha + \frac{3-\sqrt{-39}}{2}\beta : \alpha, \beta \in \mathcal{O}(\sqrt{-39})\}$

Si ara tenim $\mathcal{V} =< 2, \frac{-3-\sqrt{-39}}{2} >\in \mathcal{O}(\sqrt{-39})$, $N(\mathcal{V}) = \frac{|2\frac{-3+\sqrt{-39}}{2} - 2\frac{-3-\sqrt{-39}}{2}|}{\sqrt{-39}} = 2$. *La forma quadràtica associada és* $f_{\mathcal{V}} = \frac{(2x+\frac{-3-\sqrt{-39}}{2}y)(2x+\frac{-3+\sqrt{-39}}{2})}{2} = 2x^2 - 3xy + 6y^2 \in C(-39)$.

Per últim veiem un exemple de l'observació 1.8.

A l'exemple 1.2.14 hem vist $f_4 * f_2 = (6, 3, 2)$. *Considerem* $3\alpha + \frac{3-\sqrt{-39}}{2}\beta \in \mathcal{U}_{f_4}$ *i* $2\alpha' + \frac{1-\sqrt{-39}}{2}\beta' \in \mathcal{U}_{f_2}$ *i els multipliquem:*

$$(3\alpha+\frac{3-\sqrt{-39}}{2}\beta)(2\alpha'+\frac{1-\sqrt{-39}}{2}\beta') = 6\alpha\alpha'+\frac{3-\sqrt{-39}}{2}(2\alpha'\beta+\beta\beta'\frac{1-\sqrt{-39}}{2})+3\alpha\beta'\frac{1-\sqrt{-39}}{2} =$$

$$= 6\alpha\alpha' + \frac{3-\sqrt{-39}}{2}(2\alpha'\beta + \beta\beta'\frac{1-\sqrt{-39}}{2}) + 3\alpha\beta'\frac{3-\sqrt{-39}}{2} - 3\alpha\beta' = 6\tilde{\alpha} + \frac{3-\sqrt{-39}}{2}\tilde{\beta}$$

Per tant, $\mathcal{U}_{f_4} \cdot \mathcal{U}_{f_2} =< 6, \frac{3-\sqrt{-39}}{2} >$ *que és l'ideal associat a* $(6, 3, 2)$.

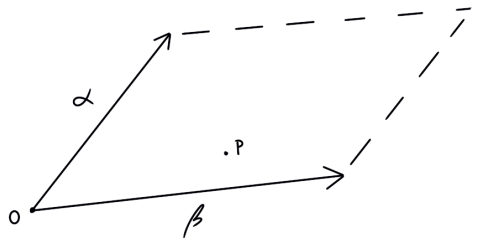
2 Una pinzellada sobre superfícies abelianes

2.1 Superfícies abelianes definides sobre $\mathbb{C}$

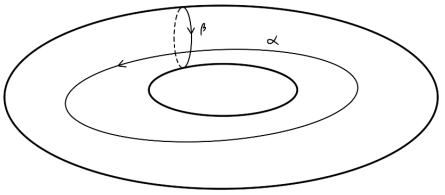
Diem que una *varietat abeliana sobre* $\mathbb{C}$ és $\mathbb{C}^g/\Lambda$, on Λ és una xarxa amb un producte complint certes propietats amb $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}^g$ i g és la dimensió, podeu trobar la definició precisa a [15, p.19].

Definició 2.1.1. Una *corba el·líptica sobre* $\mathbb{C}$ és una varietat abeliana de dimensió 1 sobre $\mathbb{C}$. Escriurem les corbes el·líptiques sobre $\mathbb{C}$ com $C = \mathbb{C}/\Lambda$ on Λ és una xarxa en $\mathbb{C}$ generada per $\alpha, \beta \in \mathbb{C}$ que són linealment independents sobre $\mathbb{R}$, $\Lambda =< \alpha, \beta >$

Observació 2.1. *Identificant els costats oposats del paral·lelogram* $O, \alpha, \alpha+\beta, \beta$*, (2.1a), obtenim el tor C (2.1b). Les imatges de les rectes* $\overline{O\alpha}$ *i* $\overline{O\beta}$*, son camins tancats sobre el tor, denotades també per* α *i* β*.*



(a) Paral·lelogram de la xarxa $\Lambda =< \alpha, \beta >$



(b) Tor generat per Λ i els camins α i β sobre el tor

Figura 2.1: Corba el·líptica sobre $\mathbb{C}$

Definició 2.1.2. Una *isogènia* és un morfisme de grups algebraics que és exhaustiva i té nucli finit.

Donades E_1 i E_2 corbes el·líptiques, una isogenia entre E_1 i E_2 és un morfisme $\phi : E_1 \longrightarrow E_2$ satisfent $\phi(O_{E_1}) = O_{E_2}$ i $\phi(E_1) \neq \{O_{E_2}\}$.

E_1 i E_2 són *isògenes* si $\exists\phi$ isogènia entre elles.

Podem prendre Λ tal que $\Lambda =< 1, \tau >$ amb $Im(\tau) > 0$[1], escriurem Λ_τ.

Lema 2.1.1. *Per* τ, τ' *del semiplà superior, es té que* $\mathbb{C}/\Lambda_\tau$ *i* $\mathbb{C}/\Lambda_{\tau'}$ *són isomorfes si i només si* $\exists a, b, c, d \in \mathbb{Z}$ *amb* $ad - bc = 1$ *tal que* $\tau' = \frac{a\tau+b}{c\tau+d}$*, veieu [18].*

[1]Per [18, Th.4.1], Λ i Λ_τ seràn isomorfes quan hi hagi una isogènia entre C i $C_\tau = \mathbb{C}/\Lambda_\tau$ i $\exists\gamma \in \mathbb{C}^*$ tal que $\Lambda = \gamma\Lambda_\tau$. Podem escollir α tal que normalitzi Λ_τ.

Diem que $\mathbb{C}/\Lambda_\tau$ serà de *multiplicació complexa* si $\tau \in \mathbb{Q}(\sqrt{D})$ per a cert $D < 0$. Això té relació amb l'anell d'endomorfismes de corbes el·líptiques però no hi entrarem en aquest treball, veieu [18, p.100]

Definició 2.1.3. Una *superfície abeliana complexa* és una varietat abeliana de dimensió 2 sobre $\mathbb{C}$.

Definició 2.1.4. Es diu que G és una superfície abeliana complexa *singular*, seguint [17], si G és isogènia al producte $C \times C$, on C és una corba el·líptica amb multiplicació complexa. Equivalentment G és singular si és el producte $C_1 \times C_2$ on C_1 i C_2 són corbes el·líptiques mutuament isogènies amb multiplicació complexa. (Consulteu [17, §4] per més detalls)

Observació 2.2. *Segons l'article [17], podem pensar G una superfície abeliana singular com $\mathbb{C}^2/\Lambda \cong \mathbb{C}/ < 1, \tau_1 > \times \mathbb{C}/ < 1, \tau_2 >$, amb Λ una xarxa de rang 4 i*

$$\tau_1 = \frac{-b + \sqrt{d}}{2a},\ \tau_2 = \frac{b + \sqrt{d}}{2}$$

on $a, b \in \mathbb{Z}$ i $0 > d = b^2 - 4ac$ per un cert c enter.

Definició 2.1.5. Sigui G una superfície abeliana, tenim un homomorfisme:

$$P_G : H^2(G, \mathbb{Z}) \longrightarrow \mathbb{C}$$

únicament definit excepte pel producte d'una constant. Entenem $H^i(G, \mathbb{Z})$ com el producte exterior de i 1-formes diferencials, veieu l'observació següent pel càlcul de P_G. Anomenem P_G l'*aplicació de 2-períodes* de G.

Definim també la *xarxa transcendental* de G com $T_G = Ker(P_G)^\perp$.

Teorema 2.1.2. *Siguin X i Y dues superfícies abelianes i assumint que $X = \mathbb{C}/\Lambda_{\tau_1} \times \mathbb{C}/\Lambda_{\tau_2}$. Suposem que existeix una isometria (isomorfisme preservant el producte escalar):*

$$\phi : H^2(X, \mathbb{Z}) \xrightarrow{\sim} H^2(Y, \mathbb{Z})$$

satisfent

$$P_Y \circ \phi = k \cdot P_X$$

per k constant diferent a zero. Aleshores Y és isomorfa a X.

Demostració. Podeu trobar la demostració a [16, p.55] □

Observació 2.3.

- *Fem la identificació següent: $Hom(H^2(G, \mathbb{Z}), \mathbb{C}) = H^2(G, \mathbb{C})$.*[2]
- *Donada G una superfície abeliana representada com un tor complex $\mathbb{C}/\Lambda$, prenem $\{v_1, v_2, v_3, v_4\}$ una base de Λ i la base dual $\{u^1, u^2, u^3, u^4\}$ en Λ^*, és a dir $u^i(v_j) = \delta_{ij}$. Aleshores $\{u^i \wedge u^j | 1 \leq i < j \leq 4\}$ forma una base de $H^2(G, \mathbb{Z})$, que també és una $\mathbb{C}$-base de $H^2(G, \mathbb{C})$ (veieu [17, p.263]). L'aplicació de 2-períodes P_G, considerat com un element de $H^2(G, \mathbb{C})$ ve donat per:*

$$P_G = \sum_{i<j} \det(v_i\ v_j) u^i \wedge u^j \tag{2.1}$$

[2] Tenim 2-formes diferencials a coeficients enters i la idea és extendre-les a coeficients complexos mitjançant el "*cup product*"(en anglès). Per ampliar infomació consulteu [11].

- *La xarxa transcendental T_G determina, i ve determinada per, una classe d'equivalència de matrius parelles definides positives respecte $GL_2(\mathbb{Z})$ (veieu [17, p.262]). Prenent una base $\{t_1, t_2\}$ de T_G, associem:*

$$Q = \begin{pmatrix} t_1^2 & t_1t_2 \\ t_1t_2 & t_2^2 \end{pmatrix} = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \tag{2.2}$$

on $a, b, c \in \mathbb{Z}$ tals que $a, c > 0$ i $b^2 - 4ac < 0$.

Teorema 2.1.3. *Sigui T_G la xarxa transcendental d'una superfície abeliana singular G. Aleshores $G \longrightarrow T_G$ és exhaustiva, generalment hi ha una correspondència dos-a-un entre superficies abelianes singulars i xarxes de rang 2.*

Demostració. • Prenem una matriu $Q = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ amb $a, b, c \in \mathbb{Z}$, $a, c > 0$ i $\Delta = b^2 - 4ac < 0$.

Sigui T una xarxa de rang 2 definida per Q, per (2.2), construirem dues superfícies abelianes A i A' tals que

$$T_A \simeq T,\ T_{A'} \simeq T.$$

Prenem $\tau_1 = \frac{-b+\sqrt{\Delta}}{2a}$, $\tau_2 = \frac{b+\sqrt{\Delta}}{2}$ i escrivim

$$C_i = \mathbb{C}/ < 1, \tau_i >,\ i = 1, 2$$

Considerem la superfíce abeliana $A = C_1 \times C_2 = \mathbb{C}^2/\Lambda$ on Λ és una xarxa de $\mathbb{C}^2$ generada per

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ v_3 = \begin{pmatrix} -\tau_1 \\ 0 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ \tau_2 \end{pmatrix}.$$

Per l'observació 2.3, prenem la base dual $\{u^j\}$ de $\{v_i\}$ i escrivim $u^{ij} = u^i \wedge u^j$. Observem que $u^{12} \wedge u^{34} = 1$ sota la identificació natural de $H^4(A, \mathbb{Z}) = \mathbb{Z}$.

Utilitzant (2.1) tenim:

$$P_A = u^{12} + cu^{34} + \tau_1 u^{23} + \tau_2 u^{14} \tag{2.3}$$

Calculem ara $Ker(P_A)$ i $Ker(P_A)^\perp$, posem $\{s_i\}$ la base de $Ker(P_A)$ i $\{t_j\}$ la base de $Ker(P_A)^\perp$.

$$\begin{cases} s_1 = u^{13} \\ s_2 = u^{42} \\ s_3 = u^{23} - au^{14} - bu^{34}s_4 = u^{12} - cu^{34} \end{cases} \qquad \begin{cases} t_1 = u^{23} + au^{14} \\ t_2 = bu^{14} + u^{12} + cu^{34} \end{cases} \tag{2.4}$$

Fent els següents càlculs:

$$\begin{aligned} t_1^2 = (u^{23} + au^{14})^2 = au^{23}u^{14} + au^{14}u^{23} = 2au^{12} \wedge u^{34} = 2a \\ t_1t_2 = (u^{23} + au^{14})(bu^{14} + u^{12} + cu^{34}) = bu^{23}u^{14} = bu^{12} \wedge u^{34} = b \\ t_2^2 = (bu^{14} + u^{12} + cu^{34})^2 = cu^{12}u^{34} + cu^{34}u^{12} = 2cu^{12} \wedge u^{34} = 2c \end{aligned}$$

podem confirmar que A satisfà $T \simeq T_A$.

Substituint τ_1 i τ_2 pels seus conjugats $\overline{\tau_1}, \overline{\tau_2}$ obtenim una altra superfície abeliana $A' = C_1' \times C_2'$, on $C_1' = \mathbb{C}/ < 1, \overline{\tau_i}$. Seguint el mateix argument veiem $T_{A'} \simeq T$. Observem que $P_{A'} = \overline{P_A}$.

- Sigui X una superfície abeliana singular tal que $T_X \simeq T$, on T és una xarxa euclidiana definida per Q, demostrarem que
$$X \simeq A \text{ o bé } X \simeq A'. \tag{2.5}$$
Suposem que tenim una isometria $\phi_0 : T_A \simeq T_X$. Pel Teorema 1 de ([17], Appendix), ϕ_0 el podem extendre a una isometria
$$\phi : H^2(A,\mathbb{Z}) \xrightarrow{\sim} H^2(A,\mathbb{Z}),\ \phi|_{T_A} = \phi_0.$$
Siguin P_X i P_A les aplicacions de 2-períodes de X i A, aleshores P_A i $P_X \circ \phi$ en $H^2(A,\mathbb{Z})$ tenen la propietat:
$$\begin{cases} P^2 = 0 \\ P\overline{P} > 0 \\ P|_{T_A^\perp} = 0 \end{cases}$$
Per la Proposició 2 de ([17], Appendix), tenim unicitat de P, per tant
$$P_X \circ \phi = \begin{cases} k \cdot P_A \\ k \cdot \overline{P_A} = k \cdot P_{A'} \end{cases} \tag{2.6}$$
per k constant no zero. A i A' són productes de dues corbes el·líptiques, pel Teorema 2.1.2 aplicat a (2.6) obtenim
$$X \simeq A \text{ o bé } X \simeq A'$$

Queda així demostrat el teorema.

□

Definició 2.1.6. Diem que una forma binària quadràtica és *parella* si la podem escriure com $f = 2(a,b,c)$ amb $a,b,c \in \mathbb{Z}$ i (a,b,c) és definida positiva.

Teorema 2.1.4 (Shioda)**.** *Les superfícies abelianes singulars estan en correspondència un-a-un amb les classes d'equivalència respecte $SL_2(\mathbb{Z})$ de formes quadràtiques binàries parelles .*

Demostració. Denotem per A_Q la superfície abeliana $A = C_1 \times C_2 = \mathbb{C}^2/\Lambda$ definida a la demostració del teorema anterior.

Si substituïm Q per
$$Q' = M^T Q M,\ M \in SL_2(\mathbb{Z})$$
Els punts τ_1, τ_2 queden substituïts per τ_1', τ_2' tals que
$$\tau_1' = M^{-1}\tau_1 = \frac{\alpha\tau_1 + \beta}{\gamma\tau_1 + \delta},\ M^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$
$$\tau_2' = \tau_2 + n,\ n \in \mathbb{Z}$$

L'expressió de τ_2' ve determinada per la de τ_1', es pot comprovar que $\tau_2 = b + a\tau_1$, utilitzant aquesta relació i desenvolupant els càlculs arribem a $\tau_2' = \tau_2 + n,\ n \in \mathbb{Z}$.

Per tant, la classe d'isomorfismes de la superfície abeliana A_Q depen únicament de la classe d'equivalència de Q respecte $SL_2(\mathbb{Z})$.

Observem que A' de la demostració del Teorema 2.1.3 es pot escriure com
$$A' = A \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} Q \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.7}$$

Denotem per $\mathcal{S}$ el conjunt de totes les matrius 2×2 parelles definides positives Q i $\mathcal{S}/SL_2(\mathbb{Z})$ o $\mathcal{S}/GL_2(\mathbb{Z})$ les classes d'equivalència d'$\mathcal{S}$ respecte $SL_2(\mathbb{Z})$ o $GL_2(\mathbb{Z})$.

Aleshores tenim el següent diagrama commutatiu:

$$\begin{array}{ccc} \mathcal{S}/SL_2(\mathbb{Z}) & \xrightarrow{\quad f \quad} & \{\text{superfícies abelianes singulars}\}/\text{isom.} \\ {\scriptstyle \text{natural}}\downarrow & & \downarrow{\scriptstyle g} \\ \mathcal{S}/GL_2(\mathbb{Z}) & \xrightarrow{1:1} & \{\text{xarxes euclidianes definides positives de rang 2}\}/\text{isom} \end{array} \tag{2.8}$$

on f i g són les aplicacions induïdes per:

$$Q \longrightarrow A_Q \text{ i } X \longrightarrow T_X$$

De (2.5) i (2.7) concloem que f és exhaustiva.

Per acabar la demostració només cal veure que f és injectiva.

Assumim

$$A_Q \simeq A_{Q^*} \text{ per } Q, Q^* \in \mathcal{S}$$

Per (2.8) tenim

$$Q \sim Q^* \text{ respecte } GL_2(\mathbb{Z}). \tag{2.9}$$

Pel teorema anterior tenim

$$C_1 \simeq C_1^* = \mathbb{C}/ < 1, \tau_1^* >$$

on τ_1^* ve definida per Q^* de la mateixa manera que τ_1 per Q. τ_1 i τ_1^* són punts equivalents al semiplà superior sota $SL_2(\mathbb{Z})$. Si denotem Q_0 (o Q_0^*) la part parella "primitiva"de Q (o Q^*), és a dir

$$\begin{cases} Q_0 = \begin{pmatrix} 2a_0 & b_0 \\ b_0 & 2c_0 \end{pmatrix}, & mcd(a_0, b_0, c_0) = 1 \\ Q = mQ_0, & \text{per algun enter } m \geq 1 \end{cases}$$

i de manera similar per Q^*, implica que

$$Q_0 \sim Q_0^*, \text{ respecte } SL_2(\mathbb{Z}) \tag{2.10}$$

Combinant (2.9) i (2.10) concloem que Q i Q^* són equivalents respecte $SL_2(\mathbb{Z})$

Per últim, recordem que a una matriu definida positiva parella Q li podem associar una forma binària quadratica. Si la matriu és parella i definida positiva, la forma també ho serà:

$$Q = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \longleftrightarrow F_Q(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

□

Exemple 2.1.5. *Veiem un exemple del Teorema 2.1.4 utilitzant els procediments de les demostracions dels Teoremes 2.1.3 i 2.1.4.*

- *Prenem* $f = 2(1, 1, 22)$ *que és una forma parella. Escrivim*

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 44 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

i associem la matriu $Q_f = \begin{pmatrix} 2 & 1 \\ 1 & 44 \end{pmatrix}$ *a la forma* f. *Per (2.2) associem* Q *a una xarxa transcendental* $T_f = \{t_1, t_2\}$ *de manera que*

$$Q_f = \begin{pmatrix} 2 & 1 \\ 1 & 44 \end{pmatrix} = \begin{pmatrix} t_1^2 & t_1 t_2 \\ t_1 t_2 & t_2^2 \end{pmatrix}$$

Construïm ara una superfície abeliana singular A_f *de manera que* $T_{A_f} \simeq T_f$. *Per la demostració del Teorema 2.1.3 si*

$$\tau_1 = \frac{-1+\sqrt{-87}}{2},\ \tau_2 = \frac{1+\sqrt{-87}}{2}$$

Definim $C_i = \mathbb{C}/ < 1, \tau_i >$, $i = 1, 2$ *i* $A_f = C_1 \times C_2$. *Per* A_f *construïda d'aquesta manera* $T_{A_f} \simeq T_f$ *i, per tant, podem associar* A_f *a la forma* f.

- *Considerem ara* $A' = \mathbb{C}/ < 1, \tau_1' > \times \mathbb{C}/ < 1, \tau_2' > = \mathbb{C}^2/\Lambda$ *per*

$$\tau_1' = \frac{2+\sqrt{-68}}{6},\ \tau_2' = \frac{-2+\sqrt{-68}}{2}$$

amb $(-2)^2 - 4 \cdot 3 \cdot c = -68 \Longrightarrow c = 6$. *Definim*

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ v_3 = \begin{pmatrix} -\frac{2+\sqrt{-68}}{6} \\ 0 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ \frac{-2+\sqrt{-68}}{2} \end{pmatrix}.$$

on $\{v_k\}$ *és una base de* Λ. *Considerant* $\{u^i\}$ *la base dual de* $\{v_k\}$ *i* $u^{ij} = u^i \wedge u^j$ *definim l'aplicació de 2-períodes de* A' *segons (2.3):*

$$P_{A'} = u^{12} + 6u^{34} + \frac{2+\sqrt{-68}}{6}u^{23} + \frac{-2+\sqrt{-68}}{2}u^{14}$$

i per (2.4) trobem la base $\{t_1', t_2'\}$ *de* $T_{A'}$*:*

$$\begin{cases} t_1 = u^{23} + au^{14} \\ t_2 = bu^{14} + u^{12} + cu^{34} \end{cases}$$

Per (2.2) associem una matriu $Q_{A'}$ *a la xarxa transcendental* $T_{A'}$*:*

$$Q_{A'} = \begin{pmatrix} t_1^2 & t_1 t_2 \\ t_1 t_2 & t_2^2 \end{pmatrix} = \begin{pmatrix} 6 & -2 \\ -2 & 12 \end{pmatrix}$$

Per últim definim $f_{A'}(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} 6 & -2 \\ -2 & 12 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ *la forma parella associada a* A', $f_{A'} = 2(3, -2, 6)$.

Observació 2.4. *Donada una superfície abeliana complexa singular* $A = \mathbb{C}^2/\Lambda = C_1 \times C_2$ *on* $C_i = \mathbb{C}/ < 1, \tau_i >$ *per* $i = 1, 2$ *i* τ_i *segons l'observació 2.2, cada corba té una 1-forma holomorfa* $dz^i = dx^i + \tau_i dy^i$, $0 \leq x^i, y^i \leq 1$. *Observem que la combinació de productes exteriors de* dx^i *i* dy^i, $i = 1, 2$, *forma una base dual per* Λ.

Considerem ara la $(2, 0)$ *forma* $\Omega = dz^1 \wedge dz^2$*:*

$$\Omega = dz^1 \wedge dz^2 = (dx^1 + \tau_1 dy^1) \wedge (dx^2 + \tau_2 dy^2) = (dx^1 + \tau_1 dy^1) \wedge (dx^2 + \tau_2 dy^2) =$$

$$= dx^1dx^2 + \tau_2 dx^1dy^2 + \tau_1 dy^1dx^2 + \tau_1\tau_2 dy^1dy^2$$

Notem que $\tau_2 = b + a\tau_1$ *i* $\tau_1\tau_2 = -c$*, substituint:*

$$\Omega = dx^1dx^2 + bdx^1dy^2 + a\tau_1 dx^1dy^2 + \tau_1 dy^1dx^2 - cdy^1dy^2 =$$
$$(dx^1dx^2 + bdx^1dy^2 - cdy^1dy^2) + \tau_1(adx^1dy^2 + dy^1dx^2) = t_2 + \tau_1 t_1$$

Les 2-formes t_1, t_2 *són una base de la xarxa transcendental de* A *[12, p.32],* T_A*. Considerem la 4-forma* $dx^1 \wedge dy^1 \wedge dx^2 \wedge dy^2$ *que l'identifiquem a* 1 *en* $H^4(A, \mathbb{Z}) = \mathbb{Z}$ *, podem comprovar*[3]*:*

$$\begin{cases} t_1^2 = (adx^1dy^2 + dy^1dx^2)^2 = adx^1dy^2dy^1dx^2 + ady^1dx^2dx^1dy^2 = \\ \quad = -adx^1dy^1dy^2dx^2 - ady^1dx^1dx^2dy^2 = 2adx^1dy^1dx^2dy^2 = 2a \\ t_1t_2 = (adx^1dy^2 + dy^1dx^2)(dx^1dx^2 + bdx^1dy^2 - cdy^1dy^2) = \\ \quad = bdy^1dx^2dx^1dy^2 = -bdy^1dx^1dx^2dy^2 = bdx^1dy^1dx^2dy^2 = b \\ t_2^2 = (dx^1dx^2 + bdx^1dy^2 - cdy^1dy^2)^2 = -cdx^1dx^2dy^1dy^2 - cdy^1dy^2dx^1dx^2 = \\ \quad = cdx^1dy^1dx^2dy^2 + cdy^1dx^1dy^2dx^2 = 2cdx^1dy^1dx^2dy^2 = 2c \end{cases}$$

Per tant, podem fer la següent associació $u_1 = dx^1, u_2 = dx^2, u_3 = dy^1, u_4 = dy^2$ *on* $\{u_i\}$ *és la base dual per* Λ *seguint la demostració del Teorema 2.1.3 i trobem la mateixa base de* T_A*. Hem vist un mètode equivalent per calcular la base de la xarxa transcendental* T_A*.*

[3]Per simplificar escrivim $ds^i \wedge dr^j$ com $ds^i dr^j$ per $s, r = x, y$ i $i, j = 1, 2$.

Bibliografia

[1] Nathan Benjamin et al. "Black holes and class groups". A: *Research in the Mathematical Sciences* 5.4 (2018), pàg. 1 - 22.

[2] Duncan A Buell. *Binary quadratic forms: classical theory and modern computations*. Springer Science & Business Media, 1989.

[3] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Vol. 34. John Wiley & Sons, 2011.

[4] Leonard Eugène Dickson. *Introduction to the Theory of Numbers: Leonard Eugene Dickson*. University of Chicago Press, 1931.

[5] Daniel E Flath. *Introduction to number theory*. American Mathematical Soc., 2018.

[6] Albrecht Fröhlich i Martin J Taylor. *Algebraic number theory*. 27. Cambridge University Press, 1991.

[7] Carl Friedrich Gauss. *Disquisicions aritmètiques*. Institut d'Estudis Catalans, 1996.

[8] Dorian Goldfeld. "A simple proof of Siegel's theorem". A: *Proceedings of the National Academy of Sciences* 71.4 (1974), pàg. 1055 - 1055.

[9] Dorian Goldfeld. "Gauss' class number problem for imaginary quadratic fields". A: *Bulletin of the American Mathematical Society* 13.1 (1985), pàg. 23 - 37.

[10] Hans Heilbronn. "On the class-number in imaginary quadratic fields". A: *The Quarterly Journal of Mathematics* 1 (1934), pàg. 150 - 160.

[11] William G McCallum i Romyar T Sharifi. "A cup product in the Galois cohomology of number fields". A: *Duke Mathematical Journal* 120.2 (2003), pàg. 269 - 310.

[12] Gregory Moore. "Arithmetic and attractors". A: *arXiv preprint hep-th/9807087* (1998).

[13] Kathrin Schacke. "On the Kronecker product". A: *Master's thesis, University of Waterloo* (2004).

[14] François Séguin. "Composition of Binary Quadratic Forms". A: *Resonance* 24.6 (2019), pàg. 633 - 651.

[15] Goro Shimura. "Abelian varieties with complex multiplication and modular functions". A: *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton university press, 2016.

[16] Tetsuji Shioda. "The period map of abelian surfaces". A: *J. Fac. Sci. Univ. Tokyo* 25 (1978), pàg. 47 - 59.

[17] Tetsuji Shioda i Naoki Mitani. "Singular abelian surfaces and binary quadratic forms". A: *Classification of algebraic varieties and compact complex manifolds*. Springer, 1974, pàg. 259 - 287.

[18] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[19] Martin Thoma. *How to solve linear congruence equations*. 2013. URL: https://martin-thoma.com/solve-linear-congruence-equations/ (cons. 17-05-2022).

Apèndix A : Programa amb Magma per calcular formes reduïdes

```
 P<x,y> := PolynomialRing(IntegerRing(), 2);
for i in [1..100] do
    if IsDiscriminant(-i) then
        printf "D=%o\n",-i;
        printf "ClassNumber=%o\n", ClassNumber(-i);
        printf "ReducedForms=%o\n",ReducedForms(-i);
        a:=ReducedForms(-i);
        for j in [1..ClassNumber(-i)] do
            f:= a[j,1]*x^2+a[j,2]*x*y+a[j,3]*y^2;
            f;
         end for;

    end if;
end for;
```

Apèndix B : Programa amb SageMath per calcular la composició de Dirichlet

```
def ExtendedEuclideanAlgorithm(a, b):
    """
        Calculates gcd(a,b) and a linear combination such that
        gcd(a,b) = a*x + b*y

        As a side effect:
        If gcd(a,b) = 1 = a*x + b*y
        Then x is multiplicative inverse of a modulo b.
    """
    a0, b0 = a, b

    x = lasty = 0
    y = lastx = 1
    while b != 0:
        q = a / b
        a, b = b, a % b
        x, lastx = lastx - q * x, x
        y, lasty = lasty - q * y, y

    return {"x": lastx, "y": lasty, "gcd": a0 * lastx + b0 * lasty}


def solveLinearCongruenceEquations(rests, modulos):
    """
    Solve a system of linear congruences.
    """
    assert len(rests) == len(modulos)
    x = 0
    M = reduce(lambda x, y: x * y, modulos)

    for mi, resti in zip(modulos, rests):
        Mi = M / mi
        s = ExtendedEuclideanAlgorithm(Mi, mi)["x"]
        e = s * Mi
        x += resti * e
    return ((x % M) + M) % M
```

```
def dir_comp(a1,b1,c1,a2,b2,c2):
    """
    Calculates Dirichlet composition for united forms f1=(a1,b1,c1), f2=(a2,b2,c2)
    """
    D1 = b1^2-4*a1*c1
    D2 = b2^2-4*a2*c2
     """Check if the forms are positive defined and have the same discriminant"""
    if D1!=D2 or D1 > 0 or D2 > 0:
        return "The forms have different discriminant or are not positive defined"
    else:
        """Check if the forms are united"""
        while gcd(gcd(a1,a2),(b1+b2)/2) != 1 :
            if BinaryQF([a1, b1, c1]).is_reduced():
                if BinaryQF([a2, b2, c2]).is_reduced():
                    """Apply the matrix transformation (0,-1)(1,0)"""
                    a=a2
                    b2=-b2
                    a2=c2
                    c2=a
                else:
                    """Convert f2 to reduced form"""
                    Q2=BinaryQF([a2, b2, c2]).reduced_form()
                    Q2_red=Q2.polynomial().coefficients()
                    a2=Q2_red[0]
                    b2=Q2_red[1]
                    c2=Q2_red[2]
            else:
                """Convert f1 to reduced form"""
                Q1=BinaryQF([a1, b1, c1]).reduced_form()
                Q1_red=Q1.polynomial().coefficients()
                a1=Q1_red[0]
                b1=Q1_red[1]
                c1=Q1_red[2]

        A=a1*a2
        b=solveLinearCongruenceEquations([b1,b2],[2*a1,2*a2])
        B=sqrt(solveLinearCongruenceEquations([D1],[4*a1*a2]))

        C=(B^2-D1)/(4*a1*a2)
        red_form = BinaryQF([A, B, C]).reduced_form()
        return str([a1,b1,c1])+"*"+str([a2,b2,c2])+"="+str([A,B,C])
                + "=" + str(red_form.polynomial().coefficients())
```

Les funcions `ExtendedEuclideanAlgorithm()` i `solveLinearCongruenceEquations()` són extretes de [19]

Apèndix C : Taula de formes reduïdes

D	$h(D)$	Formes reduïdes
-3	1	x^2+xy+y^2
-4	1	x^2+y^2
-7	1	$x^2+xy+2y^2$
-8	1	x^2+2y^2
-11	1	$x^2+xy+3y^2$
-12	1	x^2+3y^2
-15	2	$x^2+xy+4y^2$, $2x^2+xy+2y^2$
-16	1	x^2+4y^2
-19	1	$x^2+xy+5y^2$
-20	2	x^2+5y^2, $2x^2+2xy+3y^2$
-23	3	$x^2+xy+6y^2$, $2x^2+xy+3y^2$, $2x^2-xy+3y^2$
-24	2	x^2+6y^2, $2x^2+3y^2$
-27	1	$x^2+xy+7y^2$
-28	1	x^2+7y^2
-31	3	$x^2+xy+8y^2$, $2x^2+xy+4y^2$, $2x^2-xy+4y^2$
-32	2	x^2+8y^2, $3x^2+2xy+3y^2$
-35	2	$x^2+xy+9y^2$, $3x^2+xy+3y^2$
-36	2	x^2+9y^2, $2x^2+2xy+5y^2$
-39	4	$x^2+xy+10y^2$, $2x^2+xy+5y^2$, $2x^2-xy+5y^2$, $3x^2+3xy+4y^2$
-40	2	x^2+10y^2, $2x^2+5y^2$
-43	1	$x^2+xy+11y^2$
-44	3	x^2+11y^2, $3x^2-2xy+4y^2$, $3x^2+2xy+4y^2$
-47	5	$x^2+xy+12y^2$, $2x^2+xy+6y^2$, $2x^2-xy+6y^2$, $3x^2+xy+4y^2$, $3*x^2-x*y+4*y^2$
-48	2	x^2+12y^2, $3x^2+4y^2$
-51	2	$x^2+xy+13y^2$, $3x^2+3xy+5y^2$
-52	2	x^2+13y^2, $2x^2+2xy+7y^2$
-55	4	$x^2+xy+14y^2$, $2x^2+xy+7y^2$, $2x^2-xy+7y^2$, $4x^2+3xy+4y^2$
-56	4	x^2+14y^2, $2x^2+7y^2$, $3x^2+2xy+5y^2$, $3x^2-2xy+5y^2$
-59	3	$x^2+xy+15y^2$, $3x^2+xy+5y^2$, $3x^2-xy+5y^2$
-60	2	x^2+15y^2, $3x^2+5y^2$
-63	4	$x^2+xy+16y^2$, $2x^2-xy+8y^2$, $2x^2+xy+8y^2$, $4x^2+xy+4y^2$
-64	2	x^2+16y^2, $4x^2+4xy+5y^2$
-67	1	$x^2+xy+17y^2$
-68	4	x^2+17y^2, $2x^2+2xy+9y^2$, $3x^2+2xy+6y^2$, $3x^2-2xy+6y^2$
-71	7	$x^2+xy+18y^2$, $2x^2+xy+9y^2$, $2x^2-xy+9y^2$, $3x^2+xy+6y^2$, $3x^2-xy+6y^2$, $4x^2+3xy+5y^2$, $4x^2-3xy+5y^2$
-72	2	x^2+18y^2, $2x^2+9y^2$
-75	2	$x^2+xy+19y^2$, $3x^2+3xy+7y^2$
-76	3	x^2+19y^2, $4x^2-2xy+5y^2$, $4x^2+2xy+5y^2$
-79	5	$x^2+xy+20y^2$, $2x^2+xy+10y^2$, $2x^2-xy+10y^2$, $4x^2+xy+5y^2$, $4x^2-xy+5y^2$
-80	4	x^2+20y^2, $4x^2+5y^2$, $3x^2+2xy+7y^2$, $3x^2-2xy+7y^2$
-83	3	$x^2+xy+21y^2$, $3x^2+xy+7y^2$, $3x^2-xy+7y^2$
-84	4	x^2+21y^2, $3x^2+7y^2$, $2x^2+2xy+11y^2$, $5x^2+4xy+5y^2$
-87	6	$x^2+xy+22y^2$, $2x^2+xy+11y^2$, $2x^2-xy+11y^2$, $3x^2+3xy+8y^2$, $4x^2+3xy+6y^2$, $4x^2-3xy+6y^2$
-88	2	x^2+22y^2, $2x^2+11y^2$
-91	2	$x^2+xy+23y^2$, $5x^2+3xy+5y^2$
-92	3	x^2+23y^2, $3x^2-2xy+8y^2$, $3x^2+2xy+8y^2$
-95	8	$x^2+xy+24y^2$, $2x^2+xy+12y^2$, $2x^2-xy+12y^2$, $3x^2+xy+8y^2$, $3x^2-xy+8y^2$, $4x^2+xy+6y^2$, $4x^2-xy+6y^2$, $5x^2+5xy+6y^2$
-96	4	x^2+24y^2, $4x^2+4xy+7y^2$, $3x^2+8y^2$, $5x^2+2xy+5y^2$
-99	2	$x^2+xy+25y^2$, $5x^2+xy+5y^2$
-100	2	x^2+25y, $2x^2+2xy+13y^2$

Taula C.1: Formes reduïdes per $D \in [-100, 0)$